Spunti per una riflessione sul rapporto fra biometria e processo penale - Ideas para reflexionar sobre la relación entre biometría y proceso penal - Ideas for a Reflection on the Relationship Between Biometrics and Criminal Trial

CJN

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione

IX Corso di formazione interdottorale di Diritto e Procedura penale 'Giuliano Vassalli' per dottorandi e dottori di ricerca

(AIDP Gruppo Italiano, Siracusa International Institute for Criminal Justice and Human Rights – Siracusa, 29 novembre - 1° dicembre 2018)

ISSN 2240-7618

2/2019

Editore Associazione "Progetto giustizia penale", via Altaguardia 1, Milano - c.f. 97792250157
ANNO 2019 - CODICE ISSN 2240-7618 - Registrazione presso il Tribunale di Milano, al n. 554 del 18 novembre 2011.
Impaginazione a cura di Chiara Pavesi

Diritto penale contemporaneo – Rivista trimestrale è un periodico on line ad accesso libero e non ha fine di profitto. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione. La rivista, registrata presso il Tribunale di Milano, al n. 554 del 18 novembre 2011, è edita attualmente dall'associazione "Progetto giustizia penale", con sede a Milano, ed è pubblicata con la collaborazione scientifica e il supporto dell'Università Commerciale Luigi Bocconi di Milano, dell'Università degli Studi di Milano, dell'Università di Roma Tre, dell'Università LUISS Guido Carli, dell'Universitat de Barcelona e dell'Università Diego Portales di Santiago del Cile.

La rivista pubblica contributi inediti relativi a temi di interesse per le scienze penalistiche a livello internazionale, in lingua italiana, spagnolo, inglese, francese, tedesca e portoghese. Ogni contributo è corredato da un breve abstract in italiano, spagnolo e inglese.

La rivista è classificata dall'ANVUR come rivista scientifica per l'area 12 (scienze giuridiche), di classe A per i settori scientifici G1 (diritto penale) e G2 (diritto processuale penale). È indicizzata in DoGI e DOAJ.

La rivista può essere citata in forma abbreviata con l'acronimo: *DPC-RT*, corredato dall'indicazione dell'anno di edizione e del fascicolo.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Committee on Publication Ethics).

La rivista si conforma alle norme del Regolamento UE 2016/679 in materia di tutela dei dati personali e di uso dei cookies (clicca qui per dettagli).

Ogni contributo proposto per la pubblicazione è preliminarmente esaminato dalla direzione, che verifica l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

In caso di esito positivo di questa prima valutazione, la direzione invia il contributo in forma anonima a due revisori, individuati secondo criteri di rotazione tra i membri dell'Editorial Advisory Board in relazione alla rispettiva competenza per materia e alle conoscenze linguistiche. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore.

La direzione comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se entrambe le valutazioni sono positive, il contributo è pubblicato. Se una o entrambe le valutazioni raccomandano modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se uno o entrambi i revisori esprimono parere negativo alla pubblicazione.

La direzione si riserva la facoltà di pubblicare, in casi eccezionali, contributi non previamente sottoposti alla procedura di peer review. Di ciò è data notizia nella prima pagina del contributo, con indicazione delle ragioni relative.

Se desideri proporre una pubblicazione alla nostra rivista, invia una mail a editor.criminaljusticenetwork@gmail.com. I contributi che saranno ritenuti dalla direzione di potenziale interesse per la rivista saranno sottoposti alla procedura di peer review sopra descritta. I contributi proposti alla rivista per la pubblicazione dovranno rispettare i criteri redazionali scaricabili qui.

Diritto penale contemporaneo – Rivista trimestrale es una publicación periódica *on line*, de libre acceso y sin ánimo de lucro. Todas las colaboraciones de carácter organizativo y editorial se realizan gratuitamente y no se imponen a los autores costes de maquetación y publicación.
La Revista, registrada en el Tribunal de Milan, en el n. 554 del 18 de noviembre de 2011, se edita actualmente por la asociación "Progetto giustizia penale", con sede en Milán, y se publica con la colaboración científica y el soporte de la *Università Commerciale Luigi Bocconi* di Milano, la *Università degli Studi di Milano,* la *Università di Roma Tre*, la *Università LUISS Guido Carli*, la *Universitat de Barcelona* y la *Universidad Diego Portales de Santiago de Chile.*
La Revista publica contribuciones inéditas, sobre temas de interés para la ciencia penal a nivel internacional, escritas en lengua italiana, española, inglesa, francesa, alemana o portuguesa. Todas las contribuciones van acompañadas de un breve abstract en italiano, español e inglés.
El lector puede leer, compartir, reproducir, distribuir, imprimir, comunicar a terceros, exponer en público, buscar y señalar mediante enlaces de hipervínculo todos los trabajos publicados en "Diritto penale contemporaneo – Rivista trimestrale", con cualquier medio y formato, para cualquier fin lícito y no comercial, dentro de los límites que permite la licencia *Creative Commons - Attribuzione - Non commerciale 3.0 Italia* (CC BY-NC 3.0 IT) y, en particular, debiendo mantenerse la indicación de la fuente, el logo, el formato gráfico original, así como el autor de la contribución.
La Revista se puede citar de forma abreviada cn el acrónimo *DPC-RT*, indicando el año de edición y el fascículo.
La Revista asume el Code of Conduct and Best Practice Guidelines for Journal Editors elaborado por el COPE (*Comitte on Publication Ethics*).
La Revista cumple lo dispuesto en el Reglamento UE 2016/679 en materia de protección de datos personales (clica aquí para los detalles sobre protectión de la privacy y uso de cookies).
Todas las contribuciones cuya publicación se propone serán examinadas previamente por la Dirección, que verificará la correspondencia con los temas tratados en la Revista y el respeto de los requisitos mínimos para su publicación.
En el caso de que se supere con éxito aquella primera valoración, la Dirección enviará la contribución de forma anónima a dos evaluadores, escogidos entre los miembros del *Editorial Advisory Board*, siguiendo criterios de rotación, de competencia por razón de la materia y atendiendo también al idioma del texto. Los evaluadores recibirán un formulario, que deberán devolver a la Dirección en el plazo indicado. En el caso de que la devolución del formulario se retrasara o no llegara a producirse, la Dirección se reserva la facultad de escoger un nuevo evaluador.
La Dirección comunicará el resultado de la evaluación al autor, garantizando el anonimato de los evaluadores. Si ambas evaluaciones son positivas, la contribución se publicará. Si alguna de las evaluaciones recomienda modificaciones, la contribución se publicará después de que su autor la haya revisado sobre la base de los comentarios recibidos y de que la Dirección haya verificado que tales comentarios han sido atendidos. La contribución no se publicará cuando uno o ambos evaluadores se pronuncien negativamente sobre su publicación.
La Dirección se reserva la facultad de publicar, en casos excepcionales, contribuciones que no hayan sido previamente sometidas a *peer review*. Se informará de ello en la primera página de la contribución, indicando las razones.

Si deseas proponer una publicación en nuestra revista, envía un mail a la dirección editor.criminaljusticenetwork@gmail.com. Las contribuciones que la Dirección considere de potencial interés para la Revista se someterán al proceso de *peer review* descrito arriba. Las contribuciones que se propongan a la Revista para su publicación deberán respetar los criterios de redacción (se pueden descargar aquí).

Diritto penale contemporaneo – Rivista trimestrale is an on-line, open-access, non-profit legal journal. All of the organisational and publishing partnerships are provided free of charge with no author processing fees. The journal, registered with the Court of Milan (n° 554 - 18/11/2011), is currently produced by the association "Progetto giustizia penale", based in Milan and is published with the support of Bocconi University of Milan, the University of Milan, Roma Tre University, the University LUISS Guido Carli, the University of Barcelona and Diego Portales University of Santiago, Chile.

The journal welcomes unpublished papers on topics of interest to the international community of criminal scholars and practitioners in the following languages; Italian, Spanish, English, French, German and Portuguese. Each paper is accompanied by a short abstract in Italian, Spanish and English.

For citation purposes the journal's abbreviated reference format may be used: *DPC-RT,* indicating year of publication and issue.

The journal strictly adheres to the Code of Conduct and Best Practice Guidelines for Journal Editors drawn up by COPE (Committee on Publication Ethics).

The journal complies with the General Data Protection Regulation (EU) 2016/679 (GDPR) (click here for details on protection of privacy and use of cookies).

All articles submitted for publication are first assessed by the Editorial Board to verify pertinence to topics addressed by the journal and to ensure that the publication's minimum standards and format requirements are met.

Should the paper in question be deemed suitable, the Editorial Board, maintaining the anonymity of the author, will send the submission to two reviewers selected in rotation from the Editorial Advisory Board, based on their areas of expertise and linguistic competence. The reviewers are provided with a feedback form to compile and submit back to the editorial board within an established timeframe. If the timeline is not heeded to or if no feedback is submitted, the editorial board reserves the right to choose a new reviewer.

The Editorial Board, whilst guaranteeing the anonymity of the reviewers, will inform the author of the decision on publication. If both evaluations are positive, the paper is published. If one or both of the evaluations recommends changes the paper will be published subsequent to revision by the author based on the comments received and verification by the editorial board. The paper will not be published should one or both of the reviewers provide negative feedback.

In exceptional cases the Editorial Board reserves the right to publish papers that have not undergone the peer review process. This will be noted on the first page of the paper and an explanation provided.

If you wish to submit a paper to our publication please email us at editor.criminaljusticenetwork@gmail.com. All papers considered of interest by the editorial board will be subject to peer review process detailed above. All papers submitted for publication must abide by the editorial guidelines (download here).

Nuove frontiere tecnologiche e sistema penale: alcune note introduttive

Las nuevas fronteras tecnológicas y el sistema de justicia penal: algunas notas de introducción

New Technological Frontiers and the Criminal Justice System: Some Introductory Notes

Antonio Gullo

Sommario

1. Un inquadramento generale

Quali sfide pone l'irrompere dello sviluppo tecnologico allo studioso del sistema penale? È questo l'interrogativo di fondo che ha animato il IX Corso di formazione interdottorale di Diritto e Procedura penale 'Giuliano Vassalli' per dottorandi e dottori di ricerca – dedicato a "*Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione*" e organizzato dal Gruppo Italiano dell'Associazione Internazionale di Diritto Penale insieme al *Siracusa International Institute for Criminal Justice and Human Rights* –, nonché il filo rosso dei diversi contributi, presentati e discussi in quella sede, che sono raccolti nel presente fascicolo[1].

Il binomio innovazione tecnologica e diritto penale non è certo nuovo; ed anzi ha registrato negli ultimi decenni un impulso sempre maggiore sulla scia delle interazioni tra scienza e giudice in estesi ambiti di ricostruzione delle responsabilità individuali. Del resto, quello appena evocato è proprio il titolo di un noto contributo di un Maestro delle scienze penalistiche che si interrogava sul grado di diffusione delle conoscenze scientifiche necessario (e sufficiente) per fondare un giudizio di imputazione a titolo di colpa[2].

La diffusione di *Internet* e dei *social media*, insieme alla oramai costantemente evocata rivoluzione digitale, hanno tuttavia aperto nuovi interrogativi – talvolta riproponendo, a ben vedere, temi classici ma da analizzare sotto una diversa luce in considerazione del peculiare contesto di riferimento –, così come spalancato scenari di riflessione sino a qualche anno fa inimmaginabili – si pensi all'utilizzo degli algoritmi intelligenti in diversi settori della vita e al loro impiego nei processi decisionali del giudice o, ancor prima, da parte delle agenzie di *enforcement*.

La dimensione del *cyberspazio* ha condotto alla costruzione di una categoria di reati ben

[1] Il corso si è tenuto a Siracusa nei giorni 29 novembre – 1 dicembre 2018. Il comitato scientifico che ha organizzato l'incontro è stato composto dai Proff. Vincenzo Militello, Stefano Manacorda, Gabriella di Paolo, Roberto Flor, Antonio Gullo, Vincenzo Mongillo, Nicola Pisani, Alessandro Spena e Francesco Zacchè.

[2] Marinucci (2005), p. 29 ss.

più ampia e variegata di quella dei 'tradizionali' *computer crimes*: accanto dunque a queste ultime ipotesi, su cui si registrano oramai da tempo nel nostro panorama scientifico importanti studi monografici[3], sono oggi al centro del dibattito una congerie di disposizioni criminose – si va dalla diffamazione, alla pedopornografia, a classiche fattispecie a tutela del patrimonio (truffa), sino al riciclaggio e a figure di reato cardine del diritto penale dei mercati finanziari (abusi di mercato)[4] – che, come si ricordava, in ragione dell'ambito di realizzazione sollevano interessanti e delicate questioni interpretative.

Al contempo, la centralità che assume nel contesto qui in esame il tema delle modalità di raccolta e formazione della prova – aspetti su cui non a caso insiste la Convenzione di Budapest sul *cybercrime* e che sono proprio adesso oggetto di confronto in seno al Consiglio d'Europa (si pensi alla disciplina della prova nel *cloud*) – mette bene in risalto la saldatura tra profili sostanziali e processuali, rendendo pertanto impossibile un approccio ragionato al contrasto a questi fenomeni criminali che non abbia come orizzonte il sistema penale nel suo complesso.

Infine, rimanendo ancora in un'ottica di inquadramento generale, va evidenziato come pure il settore della sicurezza informatica – per adoperare una espressione che nella sua formulazione inglese (*cybersecurity*) è oggi di moda – ha visto affermarsi, in particolare di recente, una strategia di lotta agli attacchi cibernetici imperniata anche (e in primo luogo) sulla leva preventiva: chiara testimonianza di questa mutata sensibilità sono la normativa eurounitaria in materia di *data protection* (che punta, tra l'altro, su obblighi di *compliance* e *accountability* dei soggetti destinatari della relativa disciplina)[5] e quella sulla protezione delle infrastrutture critiche (la c.d. Direttiva *NIS*) che, anche nella sua traduzione interna (d.lgs. n. 65 del 2018), ha previsto penetranti obblighi in punto di adozione di misure tecniche a carattere per l'appunto preventivo, nonché aventi ad oggetto la notifica degli eventuali *cyberattacks,* nella prospettiva di favorire cooperazione e scambio di informazioni tra gli attori coinvolti[6].

Allo stesso modo, si è iniziato a imboccare anche in questo ambito la strada, rivelatasi fruttuosa in altri settori, della cooperazione pubblico-privato e, segnatamente, del coinvolgimento delle strutture organizzative nelle logiche di *risk management* e *risk assessment,* con la delineazione altresì di meccanismi di possibile corresponsabilizzazione ai sensi del d.lgs. n. 231 del 2001 (il riferimento è al recente d.l. n. 105 del 2019 che, avuto riguardo all'implementazione del quadro di sicurezza cibernetica, ha introdotto all'interno dell'art. 24 *bis* un nuovo reato presupposto[7]).

La ricchezza del dibattito svoltosi a Siracusa e la molteplicità dei temi affrontati, in linea del resto con la composita realtà con cui bisogna oggi misurarsi, non consentono di dare conto, nel limitato spazio di queste note introduttive, di tutti i temi oggetto di analisi (che vanno dall'esame del profilo del *cybercriminale,* con la ricostruzione delle peculiarità delle condotte realizzate *on line* – in punto ad esempio di desensibilizzazione soggettiva – e l'analisi del ruolo da riservare a strumenti a carattere preventivo[8], a recenti riforme normative volte a sanzionare penalmente condotte che spesso sono realizzate *on line* – il riferimento è alla diffusione illecita di immagini o video sessualmente espliciti *ex* art. 612 *ter* c.p.– 9, a modifiche di settori di disciplina che interferiscono con le dinamiche dell'economia digitale – i reati a tutela del segreto commerciale[10] e i delitti di riciclaggio[11] –, alle ricadute che innovative modalità di raccolta del risparmio determinano sul piano dei meccanismi di controllo del mercato – il fenomeno del *crowdfounding*[12]).

Concentreremo pertanto l'attenzione su quattro aspetti in grado di intercettare altrettante questioni che attraversano trasversalmente l'area tematica qui in esame.

[3] Pecorella (2006).
[4] Su molti di questi ambiti si soffermano gli scritti qui presentati: V. Sez. I e II. Per una definizione di *cybercrime* v. Picotti (2019a), p. 75.
[5] V., *infra,* i contributi di Orlando, De Aglio, Fiorinelli e Aragona. Per un commento al Regolamento sulla protezione dei dati personali e alla normativa di recepimento interno v., D'Agostino (2019), e Manes, Mazzacuva (2019), p. 168 ss.
[6] Su questi profili v. la recente disamina di Flor (2019), p. 443 ss.
[7] Il riferimento è alla nuova fattispecie contenuta all'art. 1, comma 11, del sopra citato d.l., la quale delinea «diversi reati propri, a dolo specifico, sostanziantisi in falsità ideologiche "rilevanti" ai fini della predetta disciplina extrapenale cui è accessoria, ed in un reato di omissione propria, tutti ascrivibili solo ai soggetti – pubblici e privati – aventi sede nel territorio nazionale, che siano inclusi nel "perimetro di sicurezza nazionale cibernetica" quale definito e disciplinato da detta nuova normativa». Per un primo commento alla nuova normativa, v., Picotti – Vadalà (2019). Il decreto è stato convertito con modificazioni dalla l. n. 133 del 2019.
[8] V., *infra*, il contributo di Sestieri.
[9] Con riguardo specifico al fenomeno del *sexting*, v., *infra,* il contributo di Rosani.
[10] V., *infra*, il contributo di Omodei.
[11] V., *infra*, i contributi di Ingrao e Pomes.
[12] V., *infra*, il contributo di di Lernia.

Il primo nucleo di problemi investe gli spazi di legittimazione della libertà di espressione *on line* a fronte della tutela reclamata da altri controinteressi – ordine pubblico, reputazione, ma anche identità personale e oggi verità della notizia –, e tocca la questione dei limiti da apporre all'intervento penale in questo delicato settore.

Il secondo ambito di riflessione attiene al ruolo dei controlli sulla Rete e investe il dibattuto tema della responsabilità del *provider*, sempre oscillante tra comprensibili esigenze preventive e incombenti rischi di responsabilità di posizione. Su questa trama si innesta oggi il diverso, ma a ben vedere complementare, tema della *partnership* pubblico-privato, della proliferazione di soggetti responsabili in seno alle strutture organizzative, nonché della diffusione di obblighi di *compliance* in settori (quello della *data protection*) non ancora toccati dalla responsabilità degli enti *ex* d.lgs. n. 231 del 2001.

Il terzo contesto di analisi ha ad oggetto le interazioni tra automazione, *software* intelligenti e sistema penale: a venire qui in rilievo sono fenomeni diversi tra di loro – dall'impiego di droni in scenari di guerra o di lotta al terrorismo di matrice fondamentalista, alle c.d. *self driving cars,* al ricorso infine ad algoritmi predittivi nel processo di commisurazione della pena ad opera del giudice –, ma tutti gravidi di implicazioni teoriche e, in alcuni casi, di complesse problematiche in chiave di ricostruzione delle responsabilità dei singoli.

L'ultimo settore su ci soffermeremo riguarda l'impiego delle nuove tecnologie sul versante delle investigazioni e della raccolta della prova, con le inevitabili tensioni tra le esigenze di accertamento dei reati e i diritti fondamentali dei soggetti coinvolti.

2. La parola in Rete

Il tema della libertà di espressione *su Internet* è probabilmente quello che ha, tra i primi, richiamato l'attenzione del penalista.

Dovendo schematizzare un dibattito certamente più esteso, ci sembra che possano essere individuati alcuni ambiti di interesse.

Il primo è relativo alla esigenza di adattare la disciplina penale a tutela della reputazione – con particolare riguardo allo statuto penale della stampa – alle manifestazioni lesive dell'onore realizzate *on line*. È noto a questo riguardo l'oramai pluridecennale dibattito circa l'equiparazione delle offese in Rete a quelle realizzate a mezzo stampa e la posizione per lungo tempo contraria sia della dottrina che della giurisprudenza (che, come noto, sin dai primi anni 2000 si era indirizzata nel senso di configurare unicamente l'aggravante di cui al terzo comma dell'art. 595 c.p. *sub specie* di altro mezzo di pubblicità, in luogo dell'ipotesi di cui all'art. 13 della l. n. 47 del 1948). Ed altrettanto noto è il correlato dibattito circa l'esclusione in capo al responsabile di testate telematiche, *blog, forum* di discussione etc. delle previsioni di cui all'art. 57 c.p.[13]

Il secondo riguarda la riscoperta dei reati di opinione e della loro capacità di prestazione per contrastare il fenomeno del terrorismo di matrice fondamentalista islamica: qui si è assistito sia al riconoscimento espresso da parte del legislatore della spiccata 'pericolosità' delle condotte realizzate avvalendosi di strumenti informatici o telematici (emblema chiaro di questa tendenza è l'aggravante di cui al terzo comma dell'art. 414 c.p. introdotta dal decreto del 2015), sia alla rinascita del dibattito sulla soglia 'legittima' di anticipazione della tutela – sulla spinta anche delle indicazioni eurounitarie circa la rilevanza da conferire alle ipotesi di 'provocazione indiretta'[14].

Il terzo si inscrive sempre nell'ottica della richiesta di un maggiore intervento del diritto penale nei territori della libertà di espressione: a venire in rilievo è il dibattito, di questi tempi alquanto accesso, sulle *fake news* e, dal nostro angolo visuale, sulla possibilità/opportunità di ricorrere all'arma affilata della pena per contrastare questi fenomeni.

Infine, sono forse inquadrabili in questo contesto anche alcuni temi su cui si intrattiene qualche contributo in punto di diritto all'oblio – ambito in cui ci si confronta con un non facile bilanciamento tra tutela della *privacy* e diritto all'informazione – e di diffusione di 'processi mediatici'[15].

[13] Su entrambe le questioni, v. Seminara (2014), p. 584 ss.

[14] Nardi (2017), p. 115 ss., nonché, *infra*, il contributo di Cirillo.

[15] V., *infra*, il contributo di Mazzanti. Sul tema del difficile bilanciamento tra obblighi di segretezza ed esigenze di pubblicità nel procedimento penale, Turchetti (2014), nonché, più recentemente, Scaroina (2019).

Nel complesso la sensazione che si trae, osservando i recenti interventi normativi e gli indirizzi applicativi, è di un rafforzamento della risposta punitiva – significativo è il percorso che ha condotto, attraverso una lettura ortopedica e di tipo analogico, la giurisprudenza (sulla scia della Sezioni Unite del 2015) ad applicare la disciplina penale in materia di stampa alle testate telematiche registrate –, nonché di una propensione a dilatare gli spazi di rilevanza penale della 'parola pericolosa'[16] (tendenza, a dire il vero, più marcata nell'esperienza di ordinamenti a noi vicini – in particolare quello francese post *Charlie Hebdo*).

Anche il tema della protezione contro notizie false su *Internet* per il tramite del diritto penale è sintomatico dell'inclinazione a chiamare in causa lo strumento più incisivo e stigmatizzante per contrastare fenomeni che destano allarme sociale – in qualche misura in questa orbita si collocano le recenti disposizioni dirette a sanzionare la diffusione senza consenso di riprese etc. tra privati (sicuramente l'ipotesi di cui all'art. 617 *septies* c.p.).

Quali dovrebbero essere le soluzioni da prospettare?

Alcune questioni attengono a esigenze di revisione dell'apparato di disciplina in materia che però dovrebbero competere al legislatore: si tratterebbe dunque di mettere un punto all'infinito dibattito sulla riforma della diffamazione e compiere chiare scelte di politica criminale[17].

Altre questioni – ferma restando la problematicità di quelle incriminazioni che troppo si avvicinano ad ambiti di esercizio di diritti fondamentali – non ci sembra possano essere risolte sul piano della conformazione delle fattispecie criminose che, a fronte di beni sicuro rilievo (i quali dalla fumosa personalità dello Stato si proiettano sulla vita e incolumità fisica dei consociati), difficilmente potranno affrancarsi dalla soglia del pericolo; pericolo che non è facile tipizzare più nel dettaglio, dovendosi pertanto rimettere qui al giudice la ricerca di esiti interpretativi improntati a equilibrio, nella prospettiva di dare succo e sangue alle condotte di cui si tratta.

Sull'affidarsi infine al diritto penale, con nuove incriminazioni *ad hoc*, rispetto a condotte lesive dell'obbligo di verità delle notizie diffuse, ci pare che il crinale sia davvero pericoloso e sia piuttosto preferibile continuare a scommettere – laddove chiaramente non ricorrano figure criminose 'sperimentate' anche sul terreno della protezione dell'identità personale del soggetto, quali ad esempio la diffamazione – sulla capacità di un confronto pubblico aperto e consapevole quale strumento privilegiato per mettere a nudo le menzogne e orientare correttamente l'opinione pubblica[18].

3. Cooperazione pubblico-privato, controlli e controllori su *Internet*

La digitalizzazione dei diversi settori della vita sociale e la vulnerabilità, confermata ogni anno dai dati sugli attacchi cibernetici, delle infrastrutture deputate a governare questi settori ha comportato lo svilupparsi di una risposta articolata del legislatore.

Su questo versante è l'impresa, la struttura organizzativa complessa, uno dei principali interlocutori del legislatore; e per questa ragione si è sviluppato un approccio al contrasto a questi fenomeni che, come si accennava prima, ha attinto all'arsenale sperimentato in punto di *risk assessment e risk management* in materia di responsabilità degli enti.

Un primo settore di intervento ha dunque riguardato, accanto alla esistente previsione di cui all'art. 24 *bis* d.lgs. n. 231 del 2001 (inserita in sede di ratifica della Convenzione di Budapest sui *cybercrime)*, il fiorire di obblighi di *compliance* a carattere preventivo e muniti di, spesso piuttosto elevata, sanzione amministrativa in ipotesi di loro violazione.

L'ultimo nato in questa nuova frontiera è l'obbligo, da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali, di adottare misure tecniche per prevenire *cyberattacks*, nonché l'obbligo di notifica di eventuali attacchi, assistiti, in ipotesi di violazione, da un penetrante apparato punitivo[19]. A ben vedere presenta punti di contatto con quest'ultima scelta anche quella attuata dal legislatore europeo nel settore della protezione dei dati personali con l'oramai famoso relativo Regolamento.

[16] V. Pelissero (2015), p. 37 ss.,
[17] Sul punto sia consentito rinviare a Gullo (2016), p. 31 ss.
[18] V., *infra*, il contributo di Costantini.
[19] V., d.lgs. n. 65 del 2018 attuativo della Direttiva NIS.

Si registra difatti, come evidenziato da alcuni contributi, un fenomeno di moltiplicazione dei soggetti responsabili – il richiamo è all'inserimento accanto al titolare e al responsabile del trattamento, del *data protection officer*[20] –, nonché la costruzione di un reticolo normativo ispirato alla logica dell'*accountability e* di misure – anche qui con connotazione preventiva, affiancate da meccanismi di certificazione, codici di condotta (con riflessi anche sul piano della determinazione della sanzione) – che recano chiara traccia del collegamento con la materia della responsabilità degli enti. E pure qui si prevedono, in caso di inosservanza, risposte punitive draconiane plasmate anche in relazione alle imprese – il noto riferimento è all'ammontare di dette sanzioni, sino a dieci o venti milioni o al 2% o 4% del fatturato, su cui si è incentrata l'attenzione l'interesse dei primi commentatori[21].

Una prima risposta all'intensificarsi del fenomeno sopra descritto è dunque nel senso di superare anche qui l'idea dell'organizzazione come fattore di dispersione della responsabilità, vedendo piuttosto l'ente come alleato e la sua struttura come elemento di cooperazione nella lotta alle forme di criminalità *lato sensu* economiche.

Una seconda risposta riguarda il riaffacciarsi del tema delle 'sentinelle' su *Internet* e investe in primo luogo l'annosa questione della responsabilità del *provider*, in punto anzitutto di configurabilità a suo carico di obblighi a carattere preventivo penalmente sanzionabili *ex* art. 40 cpv.[22]

La difficoltà di trovare soluzioni appaganti è dimostrata dal fatto che si tratta di un dibattito, quest'ultimo, che si ripropone ciclicamente, nonostante anni fa la Cassazione nel caso *Google Vivi Down* sembrasse aver messo un punto fermo.

Ciò è dovuto anche a recenti pronunce della giurisprudenza di legittimità che, in ipotesi di mantenimento *on line* di materiale lesivo dell'altrui reputazione, hanno ritenuto sussistente la responsabilità del titolare di un quotidiano *on line*, non emergendo peraltro in maniera nitida se a titolo di concorso criminoso oppure in base all'art. 40 cpv.[23]. Così pure ha concorso ad alimentare il dibattito la recente direttiva eurounitaria sul contrasto al terrorismo, nonché alcune sentenze della Corte EDU (a partire da *Delfi contro Estonia*) che tuttavia, nell'un caso, fanno leva su obblighi successivi di rimozione di contenuti illeciti, e, nell'altro, si muovono sul terreno della responsabilità civile con cadenze peraltro ancora da chiarire[24].

In questo scenario non sono mancate del resto voci di studiosi autorevoli della materia che da tempo hanno reputato percorribile la strada di una responsabilizzazione del *provider ex* art. 40 cpv, valorizzando già *de iure condito* la disciplina in tema di pedopornografia[25].

Il problema ovviamente esiste e proprio le recenti tendenze normative in sede eurounitaria dimostrano come la logica della neutralità del *provider* possa (o meglio debba) a certe condizioni essere superata. In questo scenario ci sembra tuttavia che la strada più proficua sia quella di ben calibrati obblighi di eliminazione di contenuti illeciti[26], rispetto ai quali si potrebbe forse anche meditare l'introduzione di figure di reato omissivo proprio, le quali tuttavia si dovrebbero costruire in modo da tale da fugare il rischio di altrettante ipotesi di responsabilità di posizione.

4. Automazione, *software* intelligenti e sistema penale.

Il capitolo dell'analisi della trama di rapporti tra l'impiego dei più avanzati ritrovati tecnologici in numerosi settori della vita pubblica e i riflessi sul diritto sostanziale e processuale penale è probabilmente quello dotato di maggior fascino per lo studioso; ed è anche quello che si presenta con note di spiccata trasversalità.

Uno sguardo, anche rapido, ai diversi contributi inclusi nel presente fascicolo mostra come si spazi dalle questioni legate all'impiego di droni per operazioni di neutralizzazione di nuclei terroristici spesso operanti nel territorio estero (in scenari che pongono di per sé problemi di qualificazione giuridica al metro del diritto internazionale), al fenomeno delle c.d. *self driving*

[20] V., *infra*, i contributi di Fiorinelli e Aragona.
[21] D'Agostino (2019), p. 18 ss., e Manes-Mazzacuva (2019), p. 171 ss.
[22] Per un quadro del dibattito, con riferimento ai possibili ruoli del *provider*, v. Ingrassia (2012), p. 15 ss.; Seminara (2014), p. 590 ss.
[23] V., *infra*, il contributo di Panattoni nonché, volendo, Gullo (2019), p. 3920 s.
[24] V., *infra*, il contributo di Nardi.
[25] Il riferimento è, come noto, a Picotti (2007), p. 1059 ss. Più recentemente, Picotti (2019b), p. 187 ss.
[26] In questo senso, *infra*, il contributo di Nardi, che però opta per il binario amministrativo.

cars, per passare alle ulteriori multiformi potenzialità di impiego dell'intelligenza artificiale (gli scritti qui pubblicati mettono bene in evidenza la versatilità di questi strumenti: dalle piattaforme di *trading on line*, al sempre maggiore ricorso alla *data analytics* nella *criminal compliance* o, nella medesima prospettiva preventiva, in ambito tributario, sino al ruolo da assegnare agli algoritmi predittivi nel processo di determinazione della pena ad opera del giudice)[27].

E stiamo limitando lo sguardo ai profili toccati dai diversi contributi, tenuto conto che anche qui siamo in presenza di precipitati tecnologici che mostrano potenzialità di utilizzo significative anche nella fase *pre-trial* – in sede di formulazione di prognosi di pericolosità funzionali all'applicazione di misure cautelari custodiali – o nella gestione della sicurezza pubblica (il riferimento è in tal caso al settore della c.d. *predictive policing*[28]).

Il fascino di questo ambito di ricerca, al quale prima facevo cenno, è dimostrato dalle notevoli implicazioni teoriche che questi strumenti tecnologici comportano. Non sempre peraltro si tratta di battere sentieri ignoti allo studioso del diritto penale, quanto piuttosto di applicare o adattare schemi teorici consolidati alle nuove realtà di cui si tratta: non sembra del resto casuale il richiamo frequente nelle soluzioni avanzate, almeno *de iure condito*, a istituti quali l'*actio libera in causa*[29], alla teorica delle posizioni di garanzia[30], o ancora all'universo delle scriminanti[31].

Non si nasconde certo che i prossimi sviluppi tecnologici potrebbero sollevare questioni inedite – si pensi alle autovetture interamente automatizzate –, con scenari in certa misura ancora da esplorare. Così pure non si può negare – venendo a uno dei temi più toccati negli scritti, ovverosia quello del ruolo da assegnare all'intelligenza artificiale nella commisurazione della pena – come già oggi ci si debba interrogare sulla compatibilità di siffatti strumenti al metro della disciplina processuale vigente nel nostro ordinamento, nonché, in prospettiva, sulla desiderabilità, praticabilità o, più radicalmente, sulla loro stessa legittimità alla luce del quadro costituzionale di riferimento.

Il caso *Loomis,* non a caso diffusamente ricostruito e analizzato nei diversi contributi[32], ha mostrato a tutti come non di futuro si parli, bensì di una realtà incombente che non tarderà certo a presentarsi alle nostre latitudini.

E qui forse l'approccio preferibile è quello di chiedersi se davvero il ricorso agli algoritmi intelligenti contrasti con previsioni vigenti nel nostro sistema processuale – il divieto di perizia criminologia *ex* art. 220 c.p.p. – e con principi di fondo quali l'eguaglianza e la finalità rieducativa della pena. E se davvero il ruolo dell'intelligenza artificiale sia tale da soppiantare il libero convincimento del giudice.

Ancora una volta ci sembra però che la strada sia quella di tornare a confrontarsi con argomenti centrali del dibattito penalistico italiano – indagati in profondità da importanti studi monografici ampiamente richiamati negli scritti presentati[33] –, essendo al contempo supportati dalla necessaria conoscenza delle caratteristiche degli strumenti tecnologici di cui adesso tanto si parla.

5. Tecniche investigative, esigenze di accertamento dei reati e tutela dei diritti fondamentali.

L'ultima sezione dei lavori affronta, con diverse sfaccettature, una delle questioni centrali della giustizia penale odierna: il bilanciamento tra le esigenze di effettività dell'accertamento dei reati, da un lato, e quelle di salvaguardia dei diritti fondamentali dei soggetti coinvolti, dall'altro, a fronte delle amplissime – e talvolta addirittura imprevedibili – potenzialità delle nuove tecnologie sul versante probatorio.

I contributi approfondiscono quindi questa problematica dicotomia con riferimento a diversi strumenti investigativi e mezzi di prova, che spaziano dal captatore informatico, all'acquisizione di dati conservati all'interno dello *smartphone,* alla prova biometrica, e che giun-

[27] V., *infra*, i contributi di Birritteri, Cucco, Cappellini, D'Agostino.
[28] V., *infra*, il contributo di Sorbello.
[29] V., *infra*, il contributo di Palmisano.
[30] V., a proposito delle *self driving cars*, *infra*, il contributo di Cappellini.
[31] V., *infra*, il contributo di Cucco.
[32] V., *infra*, i contributi di D'Agostino, Occhiuzzi e Maldonato.
[33] V. il richiamo ai lavori di Dolcini e Mannozzi in tema di commisurazione della pena nei contributi di D'Agostino e Occhiuzzi.

gono sino alla controversa categoria dell'"atto investigativo atipico"; si affrontano altresì le questioni connesse all'accesso transfrontaliero all'"*electronic evidence*", la cui necessità è imposta dal carattere volatile e dematerializzato dei dati informatici oggetto di acquisizione[34].

L'individuazione di adeguate garanzie processuali, come si pone in evidenza, è fondamentale in ragione della particolare intrusività di tutti i mezzi citati, idonei a consentire l'accesso a una sfera – quella che comincia ad essere definita quale "domicilio informatico" – in cui sempre più si esprime la personalità dell'individuo e si sviluppano le sue relazioni sociali.

Peraltro, le molteplici modalità di possibile impiego di alcuni degli strumenti investigativi presi in esame, e in particolare del cd. "*trojan horse*", pongono il rilevante problema della previa individuazione delle libertà fondamentali incise dall'attività di accertamento, così che sia possibile enucleare le forme di relativa salvaguardia, attraverso l'imposizione di obblighi all'autorità pubblica e l'attribuzione di correlati diritti ai soggetti interessati. In questo senso, si è auspicata, accanto a un'interpretazione evolutiva degli artt. 13, 14, 15 Cost., idonea a offrire tutela alle nuove espressioni delle libertà fondamentali dagli stessi tutelate, la delineazione di un nuovo ed inedito diritto, che tenga conto degli sviluppi della personalità umana connessi all'impiego delle tecnologie informatiche. Punto di riferimento è in questo senso la decisione della Corte Costituzionale tedesca del 2008, che ha individuato il «diritto alla garanzia dell'integrità e della riservatezza dei sistemi informatici»[35].

Si è quindi preso atto dell'inadeguatezza dell'attuale sistema normativo in materia di investigazioni digitali, anche alla luce della comparazione con altri ordinamenti europei, e dell'insoddisfacente bilanciamento tra esigenze della giustizia e libertà fondamentali di cui esso è espressione; ne deriva, secondo quanto si è osservato, il rischio di intrusioni nella vita privata in contrasto con la disciplina costituzionale e sovranazionale di riferimento. Ancora una volta, tuttavia, all'approccio critico si affianca quello costruttivo, anche nella prospettiva della possibile introduzione di una regolamentazione di tutte le attività non riconducibili ad alcuna fattispecie tipica contemplata dal codice di procedura penale, così da evitare il ricorso all'ambigua figura dell'"atto investigativo atipico"[36].

L'esigenza di delineare una nuova disciplina legislativa chiarificatrice, e attenta alle istanze di protezione delle situazioni giuridiche soggettive di rilievo primario dei soggetti coinvolti, è stata altresì individuata con riguardo all'ambito della prova biometrica. Di quest'ultima si sono messe in luce le plurime espressioni, in relazione alle diverse tipologie di dati individuati in applicazione delle leggi tecnico-scientifiche, nonché i potenziali limiti; si rende pertanto necessaria una regolamentazione che, essendo calibrata su queste differenti esplicazioni, assicuri il rispetto delle garanzie processuali e una soddisfacente tutela della riservatezza[37].

La ricerca di un'appagante protezione della sfera della vita privata della persona si considera inoltre perseguibile mediante la delimitazione della tipologia di attività investigativa, e di dati acquisibili, qualora la ricerca di elementi di prova sia posta in essere su uno strumento di rilievo ormai centrale nella quotidianità di ciascuno, quale è lo *smartphone*[38].

Il problematico bilanciamento tra istanze di celerità e di efficienza nell'acquisizione degli elementi di prova, e di salvaguardia dei diritti facenti capo alla pluralità dei soggetti coinvolti, è infine oggetto di riflessione anche sotto il profilo del nuovo modello di cooperazione fondato sul contatto diretto tra l'autorità statale e il privato prestatore di servizi stabilito all'esterno della relativa giurisdizione. Tema, questo, che non interessa soltanto il contesto europeo – come testimoniato dalle recenti proposte normative della Commissione europea in materia di *electronic evidence* – ma più ampiamente lo scenario globale entro cui sono elaborati e trasferiti i dati informatici; e in questo ambito si individuano diversi livelli di tutela della riservatezza e conseguentemente di risposta alle richieste di acquisizione di elementi di prova spesso essenziali per le esigenze della giustizia penale[39].

In definitiva, la sezione conclusiva dei lavori consente di cogliere le significative e recenti istanze di pervenire a una soddisfacente regolamentazione dell'uso nel procedimento penale di strumenti tecnologici, al fine di individuarne le possibili modalità di impiego e le correlate garanzie, funzionali alla salvaguardia delle libertà fondamentali dell'individuo e alla stessa

[34] Si tratta dei contributi di Caneschi, Evaristi, Nicolicchia, Sacchetto, Tondi.
[35] V., *infra*, il contributo di Caneschi.
[36] V., *infra*, il contributo di Nicolicchia.
[37] V., *infra*, il contributo di Sacchetto.
[38] V., *infra*, il contributo di Evaristi.
[39] V., *infra*, il contributo di Tondi.

bontà dell'accertamento.

Bibliografia

Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo, Papa, Michele (eds.) (2019): *Trattato di diritto penale.* Cybercrime (Torino, Giappichelli).

D'Agostino, Luca (2019): "La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101", *Arch. pen.* (web), 1.

Flor, Roberto (2019): "*Cybersecurity* ed il contrasto ai *cyber-attacks* a livello europeo: dalla *cia-triad protection* ai più recenti sviluppi", *Diritto di Internet*, 3, p. 443 ss.

Gullo, Antonio (2016): "La tela di Penelope. La riforma della diffamazione nel Testo unificato approvato alla Camera il 24 giugno 2015", *Dir. pen. cont. - Riv. trim.*, 1, p. 31 ss.

Gullo, Antonio (2019): "*Sub* Art. 595 c.p.", Padovani, Tullio (editor), *Codice penale*, t. II, VII ed. (Milano, Giuffrè), p. 3909 ss.

Ingrassia, Alex (2012): "Il ruolo dell'Isp nel ciberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuribili di una responsabilità penale dei *provider* nell'ordinamento italiano", in Luparia, Luca (editor) (2012), *Sistema penale e criminalità informatica* (Milano, Giuffrè), p. 15 ss., consultabile anche in *Dir. pen. cont.*, 8 novembre 2012.

Luparia, Luca (2012): Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale* (Milano, Giuffrè).

Manes, Vittorio, Mazzacuva, Francesco (2019): "GDPR e nuove disposizioni penali del Codice *privacy*", *Dir. pen. proc.*, p. 168 ss.

Marinucci, Giorgio (2005): "Innovazioni tecnologiche e scoperte scientifiche: costi e tempi di adeguamento delle regole di diligenza", *Riv. it. dir. proc. pen.*, p. 29 ss.

Nardi, Valerie (2017): "La punibilità dell'istigazione nel contrasto al terrorismo internazionale", *Dir. pen. cont. - Riv. trim.*, 1, p. 115 ss.

Pecorella, Claudia (2006): *Diritto penale dell'informatica* (Ristampa aggiornata) (Padova, Cedam).

Pelissero, Marco (2015): "La parola pericolosa. Il confine incerto del controllo penale del dissenso", *Quest. giust.*, 4, p. 37 ss.

Picotti, Lorenzo (2007): "La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in *Internet* (L. 6 febbraio 2006, n. 38) (parte I e II)", *Stud. iur.*, p. 1059 ss.

Picotti, Lorenzo (2019): "Diritto penale e tecnologie informatiche: una visione d'insieme", in Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo, Papa, Michele (eds.), *Trattato di diritto penale.* Cybercrime (Milano, Utet), p. 35 ss.

Picotti, Lorenzo (2019): "La pedopornografia nel *cyberspace*: un opportuno adeguamento della giurisprudenza allo sviluppo tecnologico ed al suo impatto sociale", *Diritto di Internet*, 1, p. 187 ss.

Picotti, Lorenzo, Vadalà, Rosa Maria (2019): "Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti", *Sistema penale*, 5 dicembre 2019.

Scaroina, Elisa (2019): "Giustizia penale e comunicazione nell'era di *Twitter* tra controllo democratico e tutela dell'onore", *Arch. pen.* (web), 2.

Seminara, Sergio (2014): "voce *Internet* (dir. pen.)", *Enc. dir. Annali*, vol. VII (Milano, Giuffrè,), p. 567 ss.

Turchetti, Sara (2014): *Cronaca giudiziaria e responsabilità penale del giornalista* (Roma, Dike).

Contents

Contents

Financial cybercrime

Cibercrimen financiero

Financial Cybercrime

Contents

La tutela penale della privacy nel cyberspazio

La tutela penal de la privacidad en el ciberespacio

Criminal Law and the Protection of Privacy in Cyberspace

Contents

Contents

Contents

Il diritto penale nel cyberspazio

El derecho penal en el ciberespacio

Criminal Law in Cyberspace

Neutralization Theory: Criminological Cues for Improved Deterrence of Hacker Crimes

Teoria della neutralizzazione": tra prevenzione e repressione del cybercrime

"Teoría de la neutralización": Entre prevención y represión del cibercrimen.

Marcello Sestieri
Dottorando di ricerca presso l'Università LUISS "Guido Carli"
msestieri@luiss.it

Cybercrimes, Criminology | Reati informatici, Criminologia | Delitos informáticos, Criminología

Abstracts

Delineating a profile for hackers and for cybercrime in general is a complex task. Yet, identifying a criminological theory capable of encompassing all the various "types" of hackers has become a necessity.
The paper begins with a brief analysis of the three main macro-categories of hackers that have been defined at a scientific level (the so-called "black hat", "gray hat", and "white hat" hackers) and then proceeds to examine the compatibility of neutralization theory with the reasons behind the steep rise in cybercrime.
The said theory – developed to describe the increase in juvenile crime in the US during the 1950s – points out a series of psychological processes that lead criminals to neutralize the moral and emotional counter-thrusts to delinquency. In a modern interpretation, these processes seem like a perfect fit for issues related to cybercrime.
Through this re-proposal of neutralization theory, it becomes clear that a traditional manner of thinking of deterrence fails when it comes to repressing cybercrime, and that a multi-sectoral strategy is now required.

Svolgere un'analisi criminologica in materia di *cybercrime* è attività complessa: del resto, ad essere complessi sono i concetti stessi di criminale informatico (in generale) e di *hacker* (in particolare). Dopo aver accennato alle tre principali macro-categorie di *hackers* (*black hat, grey hat* e *white hat*), si tenterà, dunque, di individuare una teoria criminologica unitaria, in grado di sintetizzare le varie anime di tale categoria delinquenziale. In questo senso, riemergono con sorprendente attualità alcuni studi criminologici sviluppati nel secolo scorso: si allude alla c.d. "teoria della neutralizzazione", che, pur non essendo stata pensata per le tematiche relative al *cybercrime*, appare sovrapponibile a detta *species* criminosa. Secondo questa teoria, esisterebbero una serie di processi psicologici che conducono ad un azzeramento di valori al fine di neutralizzare la controspinta morale alla commissione del reato. Si dimostrerà come un simile procedimento risulti facilitato dalle caratteristiche dei reati informatici, che, dunque, si rivelano fattispecie altamente criminogene. Infine, si segnalerà come gli elementi rafforzativi della desensibilizzazione degli *hackers* riverberino altresì non trascurabili conseguenze sul più ampio tema delle funzioni della pena, depotenziando la tradizionale efficacia generalpreventiva e specialpreventiva della repressione ed imponendo al legislatore una maggiore attenzione verso rimedi preventivi di tipo alternativo.

Delinear un perfil criminológico para hackers y para el cibercrimen en general es una tarea compleja. Sin embargo, desarrollar una teoría criminológica capaz de comprender todos los "tipos" de hackers se ha vuelto una necesidad. El presente trabajo comienza con un breve análisis de las tres principales macro categorías de hackers que han

sido definidas a nivel científico (los así llamados "black hat", "gray hat" y "white hat" hackers). Posteriormente, se procede a analizar la compatibilidad de la teoría de la neutralización con las razones detrás del aumento del cibercrimen. Esta teoría, desarrollada para describir el aumento de la delincuencia juvenil en los Estados Unidos durante la década de 1950, señala una serie de procesos psicológicos que llevan a los criminales a neutralizar la moral y los obstáculos emocionales para delinquir. En base a una moderna interpretación de la teoría de la neutralización, se aprecia claramente que la manera tradicional de concebir la prevención falla cuando se trata de combatir el cibercrimen, evidenciando así la necesidad de una estrategia multisectorial.

Sommario

1. Criminology and cybercrime.

Cybercrime is an increasingly widespread phenomenon[1], and unlike the manner in which it is typically perpetrated, its effects do not remain "virtual". Indeed, cybercrime can affect not only the victims' financial situation when it is committed for financial gain, but also their fundamental rights, like privacy and security.

There are multiple factors that can favor the commission of cybercrimes, from both the victim and the offender's perspective: although these factors are certainly relevant in all traditional crimes (*e.g.* the victim's greater or lesser vulnerability, the offender's abilities and personality), when it comes to cybercrime the subjective and psychological aspects becomes surprisingly dominant[2].

Precisely because of this major role played by personal abilities and human interactions in cybercrime[3], legal scholars has extended the applicability of many criminological theories elaborated for "traditional" crimes to it, for the specific purpose of profiling hackers.

The aim of this paper is to analyze the application of one of these criminological theories – the so-called "neutralization theory" – to cybercrime, in order to find criminological cues that could guide both Italian and European legislators towards an improved deterrence strategy *vis-à-vis* this phenomenon.

2. The various facets of the "hacker phenomenon".

Carrying out a criminological analysis of cybercrime is extremely complex, as it is quite difficult to even define the concepts of "cybercrime" and "cybercriminal"[4]. Suffice it to note, for example, that legal scholars have developed a multitude of distinct criminological categories just for hackers[5]. While an exhaustive description of these categories would be too lengthy for the present purposes, some brief references to the three main macro-categories of hackers that have been defined at a scientific level will be useful: these are the so-called "black hat", "gray hat", and "white hat" hackers.

[1] Levi (2017), p. 6, points out that, according to the Office of National Statistics of the United Kingdom, in just over a year – from 2015 to March 2016 – «adults aged 16 over experienced and estimated 3.8 million incidents of fraud, with just over half of these being cyber-related». Furthermore, in Sweden – as showed by the Swedish Crime Survey of 2014 – 44% of frauds involved the Internet, while in The Netherlands, from 2010 to 2012, the cost of "identity frauds" alone was estimated at over 200 million euros.

[2] Leukfeldt (2017), p. 12, talks about a "human factor" to indicate how the offender's skills and the different level of the victim's vulnerability can affect both the choice in "target" and the frequency of the commission of computer crimes; the author defines this the "risk of cybercrime victimization".

[3] Leukfeldt *et al. (*2017), pp. 25-26, identify two main categories of attacks, with four variables depending on the intensity of the contact with the victims: low-tech attacks with a high degree of victim-attacker interaction (*e.g.* the use of e-mails or websites for phishing); low-tech attacks with a low degree of victim-attacker interaction (*e.g.* the acquisition of user credentials with a false entry field); high-tech attacks with a low degree of victim-attacker interaction (*e.g.* malware installed on the victim's computer/phone just with the click on a link); high-tech attacks without victim-attacker interaction (*e.g.* the infection hits the website directly, so that just the simple user's log-in allows the acquisition of all his data).

[4] This difficulty is well illustrated by Viano (2017), p. 3: «there is no universal accepted definition of cybercrime. Different definitions have been put forward by experts, the industry and scholars. Some have been used by various governments. They vary in their degree of specificity and breadth. Regardless of the definition, conceptualizing cybercrime raises several key questions, like where do the criminal acts take place in the real and digital worlds and with the help of which technologies; why are damaging activities undertaken; and who are the actors perpetrating the deviant acts? The "Where" of Criminal Activities, Actors, and Victims».
In addition, Coleman and Golub (2008), p. 267, note that: «there are, then, a wide variety of hacker practices that have been assembled out of a diverse collection of exemplary personalities, institutions, political techniques, critical events, and technologies. These practices are not guided by a singular hacker ethic but are instead rooted in and reveal a number of distinct but interesting genres of ethical practice».

[5] McKenzie (2006), p. 320, explains that the term "hacker" migrated from the university world (being previously connected to electrical engineering inventions) to a totally different category: «as computing became a pervasive force with the rise of the Internet, "hacking" developed a second meaning – it named the process of exploring computer networks. In many cases this was benign. The Internet was a new and not well-understood phenomenon, and hackers in this sense were explorers of this new terrain».

The black hat category is constituted by hackers who use their IT skills on an ongoing basis, with methods that tend to be illegal, in order to achieve a profit; hacking becomes an actual "profession" motivated by personal gain.

The gray hats represent an intermediate category composed of hackers who occasionally commit illegal actions, but without the stability characteristic of the black hats' activities. Typically, their actions are not aimed at personal enrichment but other goals, the main one being to benefit the internet community (*e.g.* to show the flaws in a security system). Despite their non-malicious intent, breaking the law would not be a decisive obstacle for gray hats: in fact, hackers in this category do not see themselves as criminals at all[6].

Finally, white hats are hackers who collaborate with law enforcement agencies, often as external consultants. In other words, they are "members of the security industry hired specifically to find security flaws"[7]. As such, further references in this paper to "hackers" will not include white hats: as their actions are not illegal, no criminological analysis is required for them.

3. The rebirth of neutralization theory.

Given the complexity in profiling hackers (and in delineating cybercrime in general), it would be useful, if not necessary, to identify a criminological theory capable of encompassing all the various "types" in this category of offenders. For this very reason, the most recent legal writings – especially in the US – have re-proposed neutralization theory in an effort to acknowledge the reasons behind the steep rise in cybercrime.

3.1. *Origins and characteristics.*

Neutralization theory was developed to describe the increase in juvenile crime in the US during the 1950s. Yet, in a modern interpretation[8], neutralization theory seems like a perfect fit for issues related to cybercrime.

In particular, according to this theory, there are a series of psychological processes that lead criminals to reset their individual values in order to find justifications for their behavior, with the consequence of neutralizing the moral and emotional counter-thrusts to crimes, which are committed, then, without feeling guilty, essentially in a condition of normality.

Gresham Sykes and David Matza postulated the neutralization theory[9] in 1957. Their starting point was a critique of the prevalent criminological theory at the time, according to which there is a radical opposition between the "dominant" values of society and the values adopted by young people who choose to commit crimes[10].

Sykes and Matza asserted that the focus, rather, should be on the reasons why individuals decide to break rules that they often believe in, and suggested that the answer might be a temporary lapse in the delinquent's values – a lapse which occurs solely to make it (psychologically) possible to behave in a manner which, without the neutralization activity, would never have occurred –.

According to the authors, this interior process manifests itself through five main (alternative) neutralization techniques[11]: the first is "Denial of responsibility", which allows the

[6] For more details on gray hats, see Kirsch (2014), pp. 383-405.
[7] Kirsch (2014), p. 386.
[8] Neutralization theory, as we know it today, is the result of numerous additions and interpolations, which have occurred over the years by various authors. For an in-depth analysis of these integrations, see Costello (2000), pp. 307-329.
Among the mentioned theoretical studies, one must mention Agnew and Peters (1986), p. 81. Particularly, the Authors note that, for an effective application and understanding of the neutralization theory, "two dimensions" must be identified: «the first dimension can be viewed as a predisposing factor toward deviance; the second dimension can be viewed as the situational factor that ignites the deviant act».
[9] Sykes and Matza (1957), pp. 664-670.
[10] Minor (1980), p. 112, notes that: «at least since the 1950s, theoretical explanations of crime and delinquency have been largely polarized into subcultural and anti-subcultural positions, in large part on the basis of whether the value system of delinquents was through to be fundamentally different from or fundamentally similar to that of the larger society. It was in this spirit that Sykes and Matza offered neutralization as theoretical alternatives to subcultural commitment».
[11] To these "original" five techniques, two have been added: Minor (1981), pp. 295-318, elaborated the "Defense of necessity" technique, which allows the rationalization of the criminal intent on the assumption that there are no valid possibilities other than committing crimes; while Klockars (1974) postulated the technique known as the "Metaphor of the ledger", through which one manages to tolerate a bad

offender to divert any self-responsibility, treating his own deviant acts like "accidents" and perceiving himself "as helplessly propelled into new situations".

The second is "Denial of injury", a process by which the offender justifies the crime as not having caused any harm, implicitly denying that their conduct could be considered a "*mala*" (a "wrong") but only "*quia prohibita*" ("because prohibited"). The third, "Denial of the victim", means a desensitization technique that allows offenders to tolerate the harm they cause to victims, who are seen as an enemy or simply absent or unknown.

The fourth technique is "Condemnation of the condemners", or contempt towards the authorities tasked with repressing certain crimes; crimes, in turn, are considered justifiable precisely because those authorities lack legitimation. Lastly, the fifth neutralization technique, "Appeal to higher loyalties", represents the inner reasoning that leads the offender to accept their delinquency based on the belief that they are acting for the good of the social group to which they belong[12].

All these techniques have been successively summarized, reworked, extended and incorporated into different professional and/or social contexts in order to find explanations for various deviant behaviors[13]. Some authors have even posited that the neutralization process may last even after the commission of the crime, for as long as the "reset" in values allows the offender to accept their actions and live with them[14].

3.2. *Compatibility with cybercrime.*

It is interesting to observe how, out of the five, Denial of injury, Denial of the victim and Condemnation of the condemners seem perfectly relatable to cybercrime in general, and to the hacker profile in particular. Indeed, all these psychological processes find clear correspondences in typical hacker conduct.

The gray hats category, for example, appears compatible with the Denial of injury technique: these hackers, while knowingly breaking the law, are still convinced that they are not doing anything wrong, because they perceive their actions as merely formal violations that do not actually cause any damage, and often committed to benefit the internet community (in this case, then, with an "Appeal to higher loyalties" as well).

As for Denial of the victim, one must consider that hackers tend to attack targets perceived as enemies by the internet community (*e.g.* companies that strictly protect copyrights); furthermore, cybercrimes represent the category of offences – perhaps *par excellence* – in which the victim is physically absent or unknown during their commission.

Finally, regarding Condemnation of the condemners, one can point out the obvious, *i.e.* that it is characteristic of the hacker community to despise authorities, which are usually perceived as a mere source of oppression against the opportunities that a "boundless Internet" could otherwise guarantee.

All these considerations (and therefore also the idea of devising an all-encompassing hacker profile through neutralization theory) might appear to be a purely theoretical endeav-

action, and overcome a sense of guilt, because they have always acted properly in the past.

[12] This last technique above all does not require a complete repudiation of the fundamental rules of a legal system, despite the failure to follow them. Particularly, Sykes and Matza (1957), p. 669, describe "the conflict between the claims of friendship and the claims of law".

[13] Polding (2017), p. 64, applies neutralization techniques to companies and highlights a series of interior justifications that can be used to "anesthetize one's values". Through the "appeal to higher loyalties" technique, for example, it becomes «acceptable to lie in a report about who was responsible for a business failure if one is protecting his or her own team».

Barlow *et al.* (2013), p. 146, emphasize the role of the "Denial of the victim" technique in the context of IT policy violations: «employees may choose to share a network password because they rationalize that no one is being injured as a result of their actions. […] By rationalizing their motivations, employees attempt to reduce their guilt or shame for intending to violate IT policies».

For another broad analysis of relations between neutralization theory and IT policy violations, see also Silic *et al.* (2017), pp. 1027-1037.

[14] Minor (1984), p. 996, states that: «the question boils down to this: Which came first, the delinquent act or the belief justifying it? To my mind, the assumption that delinquent acts come before justifying beliefs is the more plausible causal ordering with respect to many of the techniques of neutralizations. It is in fact in many cases difficult to imagine how the boy could subscribe to the belief without having engaged in delinquent acts. But these considerations do not require that we reject such "neutralizing" beliefs as causes of delinquency. On the contrary, since a boy may commit delinquent acts episodically over an extended period of time, there is every reason to believe that neutralizations in some sense resulting from the earlier acts are causes of later acts. In fact, if we reject, as we do here, the idea that the delinquent develops a set of beliefs that positively require delinquent behavior, then the development of a series of neutralizing beliefs is exactly what we mean by the "hardening" process that presumably occurs at some point in a delinquent career».

See also Costello (2000), p. 314.

or. However, this theory has recently resurfaced – at least in the US – precisely because of its relevance in practice, as evidenced by the statistical analyses conducted in the field of hacker profiling.

Indeed, according to estimates published by the Italian "Hacker profile project"[15], almost 60% of professional hackers claim to have started this kind of criminal activity between 10 and 15 years of age. This fact alone could bring us full-circle with neutralization theory, which – as a reminder – was originally postulated to explain an increase in juvenile delinquency. Clearly, the basic psychological processes that this theory describes are particularly impactful on younger individuals, for whom finding alternative justifications to the moral duties imposed by society is quite natural.

Another statistical result that gives an account of how effective the rationalization process is for hackers is the following: 65% of professional hackers stated that they did not even consider the possibility of being convicted because of their criminal activity[16], as if it were completely lawful, or their profession were like any other. These statistics demonstrate the existence of a normalization process which affects the cybercriminal's very awareness that they are committing a crime at all.

4. A new perspective on preventing hacker crimes.

All these reflections should push the criminal justice system towards alternative models of contrasting the hacker phenomenon. In fact, what emerges from this re-proposal of neutralization theory is that the standard or traditional manner of thinking of deterrence fails when it comes to repressing cybercrime.

Indeed, on the basis of the "eternal"[17] topic of the "multi-purpose" nature of punishment[18] – split between general deterrence[19] and special deterrence[20] – it becomes clear that the deterrent effect of punishment is scarce when it comes to cybercrime, considering that 65% of professional hackers do not even consider punishment on the assumption that, given the characteristics of cybercrime and cyberspace[21], they will never be caught by national authorities. Moreover, at a special deterrence level, it is likewise obvious that being sentenced for actions that the (cyber)offender does not even recognize as a crime might produce an effect opposite to their desired rehabilitation.

All the above considerations lead to the conclusion that, in order to effectively combat the occurrence and expansion of this type of crime, the criminal justice system should reject a merely repression-oriented perspective. As evidenced by the aforementioned statistics, simply extending traditional criminal justice enforcement to cybercrime would be completely inadequate as a deterrence method. In fact, if 59% of hackers start hacking between 10 and 15 years of age, what use could longer prison terms or new provisions in criminal codes ever have?

It follows that a multi-sectoral strategy seems to be necessity when it comes to curbing the rise in cybercrime. The most effective way to achieve this rather ambitious goal, then, should include direct action on young people's education, showing them the risks of hacking

[15] Chiesa and Ciappi (2007), pp. 84-85, point out that the cases in which the offender starts hacking after the age of twenty are very rare: only 4% of hackers began a criminal activity between 26 and 30 years of age, while just 1% did so after 40.
[16] Chiesa and Ciappi (2007), pp. 205-207.
[17] So described by Vassalli (1991), 619-656. The Author points out that, beyond deterrence purposes, it is undeniable that the primary function of punishment is to "reaffirm" the existence of the violated right, in order to "offset" the negative effects of the offender's conduct. Such reaffirmation "is separate from the punishment inflicted on the offender, so much so that it exists irrespective of whether the punishment is actually carried out".
[18] On the multi-faceted nature of criminal sanctions, see Mezzetti (2017), p. 711, but also Pulitanò (2017), p. 49.
[19] General deterrence is based on the idea that the threat of punishment can distract people from criminal behavior. Through "social disapproval", which creates an internal counter-thrust with a deterrent effect, general deterrence is able to create a "habit contrary to crime". This first aim of the criminal justice system can be viewed as the punishment's "effectiveness as a deterrent", or its dissuasive potential.
[20] Special deterrence, instead, works on an individual level: the criminal sanction tries to prevent the offender from "returning to crime", operating in a perspective of re-socialization. This purpose appears to be closely related to the rehabilitative purpose of the criminal sanction, required by Article 27(3) of the Italian Constitution.
Indeed, according to the Italian Constitutional Court, Judgment no. 236/2016, proportionality and rehabilitative purposes should support the criminal sanction at every stage: from when it is conceived in the abstract, to when it is applied in reality. With regard to this judgment, see Viganò (2017), pp. 61-66.
[21] Flor (2012), p. 1, describes a "de-timing of the activities" in order to emphasize how IT products are simultaneously opportunities for social development but also new potential forms of crime.

and explaining the criminal offences that it constitutes. Only by identifying the educational messages best suited to the age group in which this phenomenon is prevalently rooted can the criminal justice system truly be successful in preventing the birth of new cybercriminals.

Still, since justice and necessity are at the basis of the criminal sanctions system[22], legislators can never simply forego punishing perpetrators of cybercrimes; at the same time, however, legislators can no longer simply rely on typical criminal justice methods and provisions to fulfill their duty in preventing this phenomenon.

To conclude, in this day and age, intervening during the early stages of criminal behavior seems to be essential in order to curtail the process of normalization of cybercrime[23].

References

Agnew Robert and Peters Ardith (1986): "The Techniques of Neutralization: An Analysis of Predisposing and Situational Factors", *Criminal Justice and Behavior*, 13, pp. 81-97

Barlow Jordan, Warkentin Merril, Ormond Dustin and Dennis Alan (2013): "Don't Make Excuses! Discouraging Neutralization to Reduce IT Policy Violation", *Computer & Security*, 39, pp. 145-159

Chiesa Raoul and Ciappi Silvio (2007): *Profilo Hacker. La scienza del Criminal Profiling applicata al mondo dell'hacking* (Milano, Apogeo); Coleman Gabriella and Golub Alex (2008): "Hacker practice. Moral Genres and the Cultural Articulation of Liberalism", *Anthropological Theory*, 8, pp. 255-277

Costello Barbara (2000): "Techniques of Neutralization and Self-esteem: a Critical Test of Social Control and Neutralization Theory", *Deviant Behavior*, 21, pp. 307-329; Flor Roberto (2012): "Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet", *Diritto penale contemporaneo*, pp. 1-13

Kirsch Cassandra (2014): "The Gray Hacker: Reconciling Cyberspace Reality and the Law", *Northern Kentucky Law Review*, 41, pp. 383-405

Klockars Carl (1974): *The Professional Fence* (New York, Free Press); Leukfeldt Rutger (2017): *The Human Factor in Cybercrime and Cybersecurity* (The Hague, Eleven International Publishing)

Leukfeldt Rutger, Kleemans Edward and Stol Wouter (2017): "A Typology of Cybercriminal Networks: from Low-tech All-rounders to High Tech Specialists", *Crime, Law and Social Change*, 67, pp. 21-37

Levi Michael (2017): "Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues", *Crime, Law and Social Change*, 67, pp. 3-20; McKenzie Wark (2006): "Hackers", *Theory, Culture & Society*, 23, pp. 320-322

Mezzetti Enrico (2017): *Diritto penale. Casi e materiali*, 2ª ed., (Bologna, Zanichelli); Minor William (1980): "The Neutralization of Criminal Offence", *Criminology*, 18, pp. 103-120

Minor William (1981): "Techniques of Neutralization: a Reconceptualization and Empirical Examination", *Journal of Research in Crime and Delinquency*, 18, pp. 295-318; Minor William (1984): "Neutralization as a Hardening Process: Considerations in the Modeling of

[22] Vassalli (1961), pp. 303-306.

[23] In particular, Barlow *et al.* (2013), p. 146, point out that: «in addition to reacting to security policy violations by applying sanctions to employees who exhibit deviant behavior, organizations must also use proactive measures to deter and prevent such abuse, including the implementation of security education, training and awareness programs. […] Improved training techniques and other communication that focus on reducing rationalization behaviors may be the key in helping employees understand that policy-breaking is neither common nor acceptable. Because neutralization techniques often are stronger than sanctions in influencing intention to violate, researchers and practitioners should combat neutralization techniques directly through persuasive communication to employees, including security training programs».

Change", *Social Forces*, 62, pp. 995-1019

Polding Brian (2017): "The Extension of Neutralization Theory to Business Ethics", *Journal of Leadership Studies*, 11, pp. 63-65

Pulitanò Domenico (2017): "La misura delle pene, fra discrezionalità politica e vincoli costituzionali", *Diritto penale contemporaneo - Rivista trimestrale*, 2, pp. 48-60

Silic Mario, Barlow Jordan and Back Andrea (2017): "A New Perspective on Neutralization and Deterrence: Predicting Shadow IT Usage", *Information & Management*, 54, pp. 1027-1037

Sykes Gresham and Matza David (1957): "Techniques of Neutralization: A Theory of Delinquency", *American Sociological Review*, 22, pp. 664-670

Vassalli Giuliano (1961): "Funzioni e insufficienze della pena", *Rivista italiana di diritto e procedura penale*, pp. 297-346

Vassalli Giuliano (1991): "La pena in Italia, oggi", in *Studi in memoria di Pietro Nuvolone*, Vol. I, (Milano, Giuffrè), pp. 619-656

Viano Emilio (2017): *Cybercrime, Organized Crime and Social Responses*, (Cham, Springer)

Viganò Francesco (2017): "Un'importante pronuncia della Consulta sulla proporzionalità della pena", *Diritto penale contemporaneo - Rivista trimestrale*, 2, pp. 61-66.

«Send nudes» Il trattamento penalistico del *sexting* in considerazione dei diritti fondamentali del minore d'età

El tratamiento penal del sexting en consideración a los derechos fundamentales de los menores de edad

The Criminalisation of Sexting Involving Underage Victims

Domenico Rosani
Dottorando di ricerca in Diritto penale ed europeo presso l'Università di Innsbruck
domenico.rosani@uibk.ac.at

Abstracts

Ai minori di età gli ordinamenti internazionale ed europeo riconoscono importanti diritti (anche) in ambito digitale, attribuendo ad essi un ambito di autodeterminazione sempre maggiore al crescere della capacità di discernimento. Tale approccio alla figura del minore non è tuttavia di facile implementazione nell'ordinamento penale. Il contributo si dedica in particolare al c.d. *sexting* tra minori, dicasi lo scambio consensuale di materiali pornografici autoprodotti. Tale relativamente nuovo fenomeno è stato inizialmente ricondotto dalla giurisprudenza italiana alle fattispecie di pedopornografia; recenti decisioni hanno tuttavia riconosciuto che esso, qualora scevro da comportamenti abusivi, non meriti una repressione penale. A tentare di ovviare alla lacuna che, in aperta violazione degli obblighi di diritto internazionale ed europeo di protezione dei minori contro l'abuso sessuale, lasciava sguarnita di appropriata tutela l'eventuale non consensuale diffusione che di tali materiali intimi si dovesse fare, è intervenuto il recentissimo art. 612-*ter* c.p. nell'ambito della riforma del c.d. "codice rosso".

Tanto a nivel internacional como europeo el ordenamiento jurídico le reconoce a los menores de edad importantes derechos (también) en el ámbito digital, asegurándoles una creciente capacidad de autodeterminación a medida que aumenta su capacidad de discernimiento. No obstante, tal aproximación a la figura del menor no es todavía de fácil implementación en el ordenamiento penal. El presente artículo se aborda el fenómeno del sexting entre menores, entendido como el intercambio consentido de material pornográfico autoproducido. Este relativamente nuevo fenómeno fue inicialmente reconducido por la jurisprudencia italiana al delito de pornografía infantil; Sin embargo, recientes sentencias han señalado que el sexting libre de comportamientos abusivos no siempre debiese merece una sanción penal. Como consecuencia, la difusión no consentida del material íntimo objeto del sexting no era adecuadamente sancionada. En un esfuerzo por remediar esta abierta violación de las obligaciones internacionales y europeas de protección de la niñez en contra del abuso, actualmente el código penal italiano prevé una disposición legal específica.

Both the international and the European legal systems acknowledge important rights of underage people (also) in the digital environment, granting them increasing autonomy according to their evolving capacities. However, an implementation of such a rights-based approach in the criminal system has so far been rather difficult. This paper focuses in particular on "sexting" among underage persons, i.e. the consensual exchange of self-produced pornographic material. This relatively new phenomenon was initially traced back by Italian case-law to the crime of child pornography. However, recent decisions have recognized that sexting, if without coercion or harassment,

does not always deserve criminal sanction. As a consequence, the non-consensual diffusion of such intimate materials as well was not appropriately punished. In an effort to remedy such an open violation of the international and European obligation to protect children against sexual abuse, a specific offence is now provided for by the Italian Criminal Code (Art. 612-ter).

Sommario

1. Il minore quale attore a pieno titolo del mondo digitale.

Ogni tre utenti di internet nel mondo, uno è minore d'età[1]. Mentre già nel 2010-2012 veniva evidenziato come possedeva un profilo su un *social media* il 38% dei bambini europei d'età tra nove e dodici anni, e il 77% di quelli fra tredici e sedici anni[2], tale percentuale è ulteriormente aumentata in anni recenti. Studi condotti tra il 2017 e il 2018 hanno rilevato come, in Italia, il 97% dei ragazzi tra quindici e diciassette anni, e il 51% dei bambini di nove e dieci anni, usino quotidianamente lo *smartphone* per accedere a internet[3]. La crescente ibridazione fra *online* e *offline* e l'aumento dell'accesso mobile alla rete rendono internet parte integrante dell'esperienza quotidiana dei minori e sempre più individuale l'uso delle risorse digitali[4].

Nonostante tale centrale rilevanza del mondo digitale per i minori, l'attenzione che il legislatore e l'ampia popolazione hanno dedicato alla figura del minore quale soggetto attivamente facente uso delle risorse tecnologiche è stata, fino in tempi recenti, piuttosto limitata. Come ad esempio evidenziato in occasione dell'approvazione, in sede europea, del regolamento generale sulla protezione dei dati personali (GDPR), il minore non viene ancora pienamente considerato quale attore dell'ambito digitale[5]. Pur se in ritardo rispetto ad altre aree del mondo, dove da più tempo le interazioni dei minori con le nuove tecnologie sono oggetto di studio[6], anche in Europa sta tuttavia formandosi un considerevole bacino di conoscenza a riguardo[7].

Similmente, per quanto particolarmente concerne l'ambito penalistico, la figura del minore su internet è stata finora analizzata soprattutto in prospettiva vittimologica. Il dibattito pubblico, e con esso le scelte politiche e normative, è infatti ancora concentrato sul minore principalmente quale vittima di reato in ambito digitale[8]. L'ampio uso che i più giovani fanno delle tecnologie informatiche fa tuttavia sì che le loro stesse condotte presentino talvolta rilevanza criminogena. Nello studio dell'inquadramento penalistico di tali condotte, un ruolo centrale rivestono le fonti di diritto europeo e internazionale, che riconoscono al minore una crescente sfera di autonomia e impongono agli Stati di tutelarlo dalle vulnerabilità proprie dell'età della crescita.

Da tale angolo prospettico, il presente contributo si propone di analizzare criticamente gli

[1] Livingstone *et al.* (2016), p. 15; la percentuale è maggiore nel Sud del mondo (tra un terzo e la metà), mentre si limita a circa un quinto degli utenti globali nel Nord.
[2] Commissione europea (2012), p. 27.
[3] Mascheroni e Ólafsson (2018), p. 5.
[4] Mascheroni e Ólafsson (2018), pp. 7 e 10.
[5] Cfr. Jasmontaite e De Hert (2015), p. 22. Il regolamento costituisce sì un positivo passo in tale dimensione – la precedente normativa UE sui dati personali ignorava del tutto i minorenni –, menzionando più volte le specificità che i più giovani presentano con riguardo alle nuove tecnologie e, nello specifico, al trattamento dei dati personali. Cionondimeno, la stesura delle relative disposizioni è avvenuta senza pienamente considerare le evidenze scientifiche, nonché senza coinvolgere né gli esperti né tantomeno consultare i minori stessi. Sul tema cfr. Byrne e Burton (2017), p. 40; Carr (2017), p. 12; Savirimuthu (2016). Sul punto si permetta di rinviare anche a Rosani (2018) e (2020), par. III.
[6] Il Canada è, ad esempio, un caso di scuola, data l'ampia e rapida diffusione che internet ha conosciuto; si vedano gli studi, in particolare di Valerie Steeves, svolti nell'ambito del progetto "Young Canadians in a Wired World (Phase III)" (tutti i *link* sono stati consultati in ultimo il 18 marzo 2019). Negli Stati Uniti il centro di ricerca Pew Research Center ha svolto varie indagini qualitative e quantitative; recentemente si v. Anderson e Jingjing (2018).
[7] Una fonte particolarmente valida è il *network* di ricerca transnazionale "EU Kids Online", coordinato dalla London School of Economics and Political Science. Si v. anche "Net Children Go Mobile", che ha concluso i propri lavori nel 2016.
[8] Per una critica nei confronti di una ricostruzione dei minori quali "*passive innocents*", anche in quanto una presunzione di innocenza infantile ("*childhood innocence*") non risulta utile all'avanzamento dei diritti dei minori in ambito digitale, Bulger *et al.* (2017), pp. 750 e 758.

sviluppi normativi e giurisprudenziali che, in Italia, hanno recentemente avuto ad oggetto il c.d. *sexting*, dicasi lo scambio consensuale di materiali autoprodotti connotati sessualmente. Rilevantissime, ma ancora povere di applicazioni concrete, risultano a proposito le recenti innovazioni apportate dalla legge c.d. "Codice rosso", che nell'agosto 2019 ha introdotto il reato di "Diffusione illecita di immagini o video sessualmente espliciti" (612-ter c.p.).

La prima parte dello scritto offrirà un quadro teorico dei diritti fondamentali del minore, sanciti a livello di diritto internazionale ed europeo, che più rilevano in proposito e che devono guidare l'interpretazione della disciplina nazionale. La seconda parte si dedicherà precipuamente al *sexting*. Tale fenomeno è stato ripetutamente ricondotto alle fattispecie di pornografia minorile, teoricamente punendo con estremo rigore delle condotte minorili il cui disvalore concreto è ben diverso da quello dei comportamenti che il legislatore giustamente intendeva sanzionare con tali disposizioni. In proposito verranno prima passati in rassegna gli sviluppi della disciplina sulla pedopornografia, ampiamente plasmata da fonti internazionali ed europee, e le decisioni giurisprudenziali che per prime hanno avuto il difficile compito di inquadrare giuridicamente il fenomeno del *sexting*. A seguire verranno quindi delineate, pur nella brevità imposta dalla sua novità, le caratteristiche salienti dell'art. 612-ter c.p. e la potenziale rilevanza dello stesso nell'impedire la diffusione non consensuale di immagini intime. In ultimo verranno offerte alcune proposte di riflessione per una possibile, futura disciplina delle circostanze di liceità del *sexting* minorile.

2. Il difficile bilanciamento in ambito digitale delle istanze di protezione e partecipazione del minore.

Due sono le prospettive che tradizionalmente caratterizzano l'analisi dei diritti dei minori nel mondo occidentale[9]. Innanzitutto v'è un obbligo di tutelare il minore e, in luce delle vulnerabilità proprie dell'età evolutiva, proteggerlo dalle varie insidie a cui è esposto. Il minore possiede infatti una limitata esperienza di vita e si trova in un importante periodo di crescita, il che determina la sua parziale capacità di valutazione del contesto sociale e di volizione. In lingua inglese, si fa generalmente riferimento a tale elemento prospettico col termine *protection*. Al contempo, tuttavia, il minore va comunque sempre considerato quale titolare di ed esercente diritti suoi propri, riconoscendogli pertanto un ambito di autonomia e la possibilità di partecipare alle scelte che lo concernono e alla vita sociale (tale elemento viene solitamente indicato come *participation*)[10]. La concezione del minore d'età quale titolare ed esercente in proprio di diritti (*rights-holder*) oltre che beneficiario di protezione si è affermata a livello internazionale in particolare a seguito dell'emanazione della Convenzione ONU sui diritti del "fanciullo"[11] del 1989 (di seguito: Convenzione ONU)[12]. In precedenza, infatti, soprattutto l'ambiente culturale anglosassone si concentrava sull'elemento della *protection*, considerando pertanto il minore principalmente quale oggetto di misure di protezione[13].

Tali due istanze, di protezione e di partecipazione, vanno bilanciate in maniera dinamica, sì da rapportarsi alla capacità di discernimento e azione effettivamente posseduta dal minore concreto. L'ambito di autonomia dello stesso deve pertanto evolversi gradualmente in corri-

[9] Per un'introduzione storica ai diritti del minore da una prospettiva italiana si v. Moro *et al.* (2019), p. 3 ss.; un'approfondita illustrazione dei fondamenti e delle specificità dei diritti dei minori a livello internazionale è offerta da Kilkelly e Liefaard (2019). Per quanto specificamente concerne il diritto penale minorile si rimanda a Bertolino (2009), p. 293 ss., Palermo Fabris *et al.* (2019) e, anche per riferimenti ad altre regioni del mondo, Decker e Marteache (2017).

[10] In aggiunta, un terzo canone di lettura è quello della fornitura al minore di determinati servizi e materiali (*provision*); cfr. Lievens (2017), p. 241. Per una similare ricostruzione teorica, che distingue tra *protection*, *emancipation and participation* e *development*, cfr. van der Hof (2016), *passim*. Sul tema si v. anche la Convenzione europea sull'esercizio dei diritti dei minori, adottata dal Consiglio d'Europa il 25 gennaio 1996 e ratificata dall'Italia con la legge 20 marzo 2003, n. 77.

[11] Questa la terminologia utilizzata dalla legge italiana di ratifica (27 maggio 1991, n. 176, "Ratifica ed esecuzione della convenzione sui diritti del fanciullo"). Cionondimeno, in tale contributo si parlerà di "minori" o "minorenni", intendendo con ciò le persone prima della maggiore età, così come previsto dall'art. 1 della stessa Convenzione ONU. L'Unicef osserva come sarebbe preferibile tradurre il termine inglese "child" (letteralmente, bambino), anziché con "fanciullo", con "bambino, ragazzo e adolescente": Unicef Italia (2004), p. 2. In ambito eurounitario, il termine "child" è divenuto nel frattempo prevalente rispetto a "minor", sebbene le corrispondenti traduzioni in italiano continuino a utilizzare "minore". Cfr. la direttiva 2011/93/UE "on combating the sexual abuse and sexual exploitation of *children* and child pornography", in italiano "relativa alla lotta contro l'abuso e lo sfruttamento sessuale *dei minori* e la pornografia minorile" (enfasi aggiunta).

[12] Per una sintetica introduzione storica agli sviluppi che hanno portato all'emanazione della Convenzione ONU del 1989 cfr. Doek (2019), 3 ss.

[13] Lamarque (2016), p. 90.

spondenza dello sviluppo delle sue competenze (*evolving capacities*). Tale tema è strettamente connesso alla questione delle soglie di età. Sebbene queste ultime permettano di differenziare la risposta legislativa a seconda dell'età, esse nondimeno rimangono problematiche da tale angolo prospettico[14]. Tali soglie presuppongono infatti che una persona di una certa età sia in grado di prendere determinate decisioni e altre più giovani non lo siano, a prescindere dalle loro competenze effettive. Sebbene spesso inevitabili per garantire il regolare funzionamento di società complesse, va ugualmente considerato come le soglie d'età previste dal diritto rivestano, al più, un carattere indicativo delle effettive capacità cognitive del minore[15]. In aggiunta, come evidenziato con riguardo alle soglie d'età previste nel regolamento sulla protezione dei dati personali, in ambito digitale risulta particolarmente critico implementare le stesse senza indulgere a forme sproporzionate di sorveglianza[16].

In generale, in ambito digitale è già il bilanciamento tra istanze di protezione e di partecipazione a presentarsi particolarmente complicato. Da una parte, i giovani possiedono spesso notevoli competenze tecniche, essendo essi ampiamente attivi *online*. Le scienze pedagogiche stanno in tal senso sempre più dedicando la propria attenzione al rilevantissimo ruolo che le risorse tecnologiche rivestono nell'età evolutiva, contribuendo in più modi allo sviluppo della personalità del bambino[17]. Per quanto ora di rilievo, esse ad esempio offrono innovative modalità per comunicare ed entrare in contatto con nuove persone, a prescindere dalle circostanze di spazio e tempo così come, in parte, dalla rispettiva età, genere e status sociale[18]. L'anonimato, perlomeno superficiale, della rete permette inoltre ai minori di esprimersi più liberamente[19]. In aggiunta, la rete consente ai minori di usufruire di un certo ambito di privacy, potendo ricercare informazioni e intrattenere comunicazioni al riparo dallo sguardo dei genitori[20].

Al contempo, tuttavia, i minori continuano a presentare quella minore capacità di apprezzamento del contesto e dei conseguenti rischi che è propria dell'età evolutiva. Tale vulnerabilità è particolarmente grave nel mondo digitale, il quale si caratterizza per delle proprietà – dicasi la persistenza temporale dei materiali caricati, la loro accessibilità svincolata da limiti spaziali e la possibilità teoricamente perenne di rintracciarli[21] – di non facile comprensione nella loro rilevanza effettiva. L'incidenza nociva delle condotte virtuali è, infatti, spesso maggiore rispetto ai loro corrispettivi non-virtuali: potenti strumenti di ricerca permettono di rinvenire i dati immessi senza limiti di spazio e tempo, mentre un contenuto, forse poco rilevante nella sua individualità, acquisisce tramite la cumulazione delle attività di ulteriori utenti un dirompente carattere nocivo. Si pensi, ad esempio, alla ripetuta "condivisione" di un testo o un'immagine all'interno di un *social media*. Le possibilità di interazione lesiva, inoltre, non rimangono confinate in un determinato spazio fisico, bensì accompagnano la vittima durante l'intera giornata (è questo il caso del *cyberbullismo*, che non si limita all'edificio scolastico durante la compresenza fisica dei soggetti)[22]. La rete viene infatti utilizzata per attività lesive e criminali anche da parte dei minori stessi. Con ciò ci si riferisce sia a fattispecie "tradizionali" eseguite tramite strumenti tecnologici (ad esempio proprio il *cyberbullyismo*), sia a relativamente nuovi fenomeni di non facile inquadramento (tra cui il *sexting*). Mentre le campagne informative ed

[14] A proposito cfr. Lansdown (2005).

[15] All'interno del codice penale italiano, decisivo è il requisito d'età dei quattordici anni *ex* artt. 97 e 98 c.p. ai fini dell'imputabilità. Tra tale soglia e la maggiore età, la capacità di intendere e volere viene accertata volta per volta. Come noto, l'ordinamento considera pure altre soglie d'età; si veda ad es. l'art. 609-quater (atti sessuali con minorenne), che richiede, da una parte, il raggiungimento dei sedici anni per gli atti sessuali compiuti con particolari categorie di persone, e dall'altra esclude la punibilità degli atti compiuti con minore infratredicenne, qualora la differenza d'età non ecceda i tre anni. Sull'imputabilità del minore cfr., in generale, Romano e Grasso (2012), pp. 74 ss.; per una prospettiva straniera e storica sul tema, Duru (2018).

[16] Cfr. Macenaite (2017), p. 440; Rosani (2020), par. III, con ulteriori riferimenti.

[17] Sul tema dell'educazione dei minori con riguardo alle tecnologie si v., in termini ampi, Unicef (2017) e Consiglio d'Europa (2017); pure il Centro comune di ricerca della Commissione europea ha pubblicato interessanti studi a riguardo: cfr., ad es., Chaudron e Eichinger (2018).

[18] Anderson e Jingjing (2018); Biolcati (2010), p. 273.

[19] Nel 2011, il 50% dei minori europei tra 11 e 16 anni intervistati nell'ambito del progetto di ricerca transnazionale "EU Kids *Online*" ha dichiarato che era più facile essere se stessi su internet rispetto a situazioni faccia a faccia: Livingstone e Ólafsson (2011), p. 1. Si noti però che una ricerca nell'ambito stesso progetto, condotta nel 2017 e vertente sulle percezioni di 1.006 ragazzi e ragazze italiani tra i 9 e i 17 anni, ha evidenziato come in tal anno in Italia soltanto il 28% degli intervistati concordava ancora con tale affermazione: Mascheroni e Ólafsson (2018), p. 16.

[20] Van der Hof (2016), p. 428. Su questi temi si v. anche Rosani (2020), par. II.

[21] Boyd (2008), p. 4.

[22] Grandi (2017), p. 51. A livello italiano, tale ultimo fenomeno ha incontrato un'importante risposta normativa tramite la legge 29 maggio 2017, n. 71, sancente "disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo". Il *sexting*, come si vedrà, è stato invece finora affrontato principalmente nell'alveo delle disposizioni preesistenti, in particolare quelle dedicate al fenomeno della pornografia minorile. Tale situazione è stata innovata dalla recentissima riforma del c.d. "Codice rosso".

educative svoltesi in anni recenti hanno contribuito ad accrescere la consapevolezza sui rischi provenienti da sconosciuti, da qualche anno gli esperti hanno rilevato come sia necessario considerare maggiormente proprio i pericoli provenienti dai coetanei[23].

In ultimo, si noti come nel mondo digitale rischi e opportunità si presentino in termini tra loro strettamente intersecati. I rischi di cui i minori sono oggetto nell'interagire con le risorse tecnologiche aumentano infatti all'accrescere delle competenze informatiche: più il minore fa uso della tecnologia, più aumenta la sua esposizione ai corrispondenti pericoli. Al contempo, tuttavia, l'esperienza che in tale contesto essi acquisiscono dovrebbe pure accrescere la loro resilienza e conseguentemente la capacità di contrapporvisi[24]. Una risposta alle situazioni di rischio che si fondasse su una generale restrizione dell'accesso dei minori ad internet lederebbe pertanto gravemente lo sviluppo della personalità del minore. L'accesso alle risorse internet e alle possibilità comunicative da esso offerte risulta infatti oggigiorno di cruciale importanza per lo sviluppo della personalità e attiene così all'ambito dei diritti fondamentali[25].

3. Inquadramento a livello internazionale ed europeo dei diritti dei minori interessati dagli sviluppi tecnologici.

Sia la Convenzione ONU, sia la Carta dei diritti fondamentali dell'Unione europea (di seguito: la Carta UE) riconoscono normativamente il minore come un titolare ed esercente diritti, a cui va attribuita una crescente sfera di autonomia all'aumentare dell'età[26]. Tale riconoscimento segna il passaggio da un approccio paternalistico alla figura del minore, concentrato unicamente sulla *protection*, a un'implementazione dell'altra, centrale stella polare del diritto minorile, la *participation* del minore alle scelte che lo concernono. La determinazione della sfera di autonomia concretamente da riconoscersi al giovane conseguirà alla capacità di discernimento dello stesso e dalle caratteristiche della decisione da prendersi[27].

Pare in proposito importante individuare, seppure a sommi capi, i diritti del minore principalmente interessati dagli sviluppi tecnologici, costituendo essi un quadro di cruciale rilevanza per l'interpretazione del diritto positivo e per l'analisi della giurisprudenza nazionale che di seguito, con precipuo riferimento al fenomeno del *sexting*, si compierà. Si noti tuttavia come il minore non soltanto possegga i diritti specificamente attribuiti ai minori di età, bensì pure tutti i diritti generalmente sanciti per "ognuno". Di seguito si porrà l'attenzione sui quattro principi cardine della Convenzione ONU, così come identificati dal Comitato ONU sui diritti dell'infanzia[28].

Il Comitato riconosce quale prima pietra angolare della Convenzione ONU il principio di non discriminazione, scaturente dall'art. 2. Questi impone agli Stati di garantire i diritti del minore "a prescindere da ogni considerazione di razza, di colore, di sesso, di lingua, di religione, di opinione politica […]". Nell'alveo di tale principio è ricondotto anche il diritto a ricevere protezione da ogni forma di violenza (art. 19), di sfruttamento sessuale e di violenza sessuale (art. 34). Gli Stati devono in particolare evitare che i minori siano incitati o costretti a dedicarsi ad attività sessuali illegali, sfruttati a fini di prostituzione o di altre pratiche sessuali illegali o a fini della produzione di spettacoli o di materiale a carattere pornografico.

[23] Lievens (2014a), p. 252, e (2014b); sul tema si v. pure Livingstone *et al.* (2014), *passim*, che tuttavia invitano ad evitare eccessivi allarmi sociali a riguardo.

[24] Livingstone *et al.* (2011), p. 2 e 43. A proposito cfr. van der Hof *et al.* (2014), *passim*.

[25] Tale rilevanza a livello di diritti fondamentali degli strumenti tecnologici è stata ad esempio evidenziata con riguardo all'art. 8 del regolamento generale per la protezione dei dati personali (GDPR), il quale – perlomeno teoricamente – richiede che i minori di 16 anni (o, a discrezionalità degli Stati, 15, 14 o 13 anni) ottengano il consenso dei genitori al trattamento dei loro dati personali. Una tale norma escluderebbe da parte consistente dei servizi digitali coloro che non possano, ovvero, anche con buone ragioni, non vogliano ottenere tale consenso parentale. Cfr., fra i vari, Jasmontaite e De Hert (2015), p. 26; Unicef (2017), p. 92 s.

[26] Sui rapporti tra Convenzione ONU e Carta UE cfr. brevemente la Spiegazione relativa all'articolo 24 — Diritti del minore, Spiegazioni relative alla Carta dei diritti fondamentali, Gazzetta ufficiale dell'Unione europea C 303 del 14 dicembre 2007, pp. 17–35.

[27] Ad esempio, gli adolescenti sono generalmente più inclini a prendere decisioni poco considerate in ambiti carichi emozionalmente, concedendo maggiore attenzione ai benefici di breve durata rispetto ai rischi: Reyna e Farley (2006), p. 33.

[28] United Nations Committee on the Rights of the Child (2003), p. 3 ss. Ci si limita qua all'analisi della Convenzione ONU e della Carta dei diritti fondamentali dell'UE, data la loro diretta rilevanza per la normativa che si analizzerà e le considerazioni che seguiranno. Si noti tuttavia come la Corte europea dei diritti dell'uomo, sebbene la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali non preveda espressamente alcun diritto dei minori, ha sviluppato una copiosa giurisprudenza a riguardo, basata in particolare sull'art. 8 della Cedu: Lamarque (2016), p. 90 ss.; per quanto riguarda specificamente il diritto alla privacy dei minori su internet, cfr. Groothius (2014).

Dopodiché, l'amplissimo diritto alla vita, alla sopravvivenza e allo sviluppo del minore (art. 6) include in sé pure un diritto all'autodeterminazione informativa, così come un diritto a godere di spazi privati dove sviluppare la propria personalità[29]. Interessati a tal proposito sono i diritti all'identità (art. 8) e alla "privacy"[30] (art. 16). Di rilievo per il presente contributo sono anche la libertà di espressione, pensiero e associazione, di cui agli artt. da 13 a 15.

Terzo, costituisce principio cardine della Convenzione ONU il diritto a essere sentito. L'art. 12 sancisce che il minore deve poter "esprimere liberamente la sua opinione su ogni questione che lo interessa, le opinioni del fanciullo essendo debitamente prese in considerazione tenendo conto della sua età e del suo grado di maturità". Tale disposizione impone sia di considerare l'opinione di un minore concreto nelle decisioni che lo concernono, sia di consultare i minori quale categoria di persone qualora siano in preparazione nuove disposizioni legali o nuove politiche che li riguardino[31].

Quarta e ultima lente prospettica è il cosiddetto "interesse superiore del bambino", sebbene tale imperante traduzione italiana non riproduca al meglio il concetto originale[32]. Il principio dei *best interests of the child* richiede di tutelare quelli che sono i principali interessi del minore, differenziando la soluzione da adottarsi a seconda delle concrete capacità della persona interessata e della situazione in cui essa si trova. Tale principio vige sia in relazione a un minore concreto, sia, quale obiettivo, per tutte le decisioni che interessino collettivamente i minori quale categoria[33]. Il carattere flessibile del concetto richiede e impone di considerare il graduale sviluppo delle competenze del minore (le già menzionate *evolving capacities*).

La Convenzione ONU dispiega una duplice rilevanza per l'ordinamento italiano. Da una parte, nonostante sia stata ratificata nel 1991 tramite legge ordinaria[34], essa costituisce parametro interposto di legittimità costituzionale[35]. In aggiunta, essa rileva pure per il tramite dell'ordinamento europeo. Come l'Italia, infatti, anche tutti gli altri Stati membri dell'Unione l'hanno sottoscritta e ratificata. Da ciò consegue che la Convenzione assurge a principio generale del diritto dell'Unione *ex* art. 6 (3) del Trattato sull'Unione Europea, imponendo pertanto il suo rispetto agli Stati nell'attuazione e applicazione del diritto europeo[36].

La stessa Carta UE, dal 2009 costituente diritto primario al pari dei Trattati, riconosce specificamente all'art. 24 i "diritti dei minori" in aggiunta ai diritti a ciascuno riconosciuti a prescindere dall'età. Tale articolo, espressamente basato sulla Convenzione ONU e in particolare sui citati artt. 3, 12 e 13[37], riconosce nei primi due capoversi che "[i] minori hanno diritto alla protezione e alle cure necessarie per il loro benessere. Essi possono esprimere liberamente la propria opinione. Questa viene presa in considerazione sulle questioni che li riguardano in funzione della loro età e della loro maturità". In aggiunta, "[i]n tutti gli atti relativi ai minori, siano essi compiuti da autorità pubbliche o da istituzioni private, l'interesse superiore del minore deve essere considerato preminente".

Il diritto del minore ad essere sentito e a co-determinare la propria esistenza, in maniera sempre maggiore al crescere della capacità di discernimento, riveste così espressa, centrale importanza anche per l'ordinamento europeo[38]. Stesso dicasi per gli ordinamenti nazionali, richiesti di rispettare la Carta UE quando attuano il diritto dell'Unione[39]. La centrale rilevanza di tale principio si accompagna tuttavia troppo spesso a un generale disinteresse nelle effettive scelte legislative; il processo legislativo che ha portato alla recente riforma del "Codice rosso",

[29] Van der Hof (2016), pp. 427 e 433.
[30] Propriamente: il diritto del minore a non essere "oggetto di interferenze arbitrarie o illegali nella sua vita privata, nella sua famiglia, nel suo domicilio o nella sua corrispondenza, e neppure di affronti illegali al suo onore e alla sua reputazione".
[31] United Nations Committee on the Rights of the Child (2003), p. 5; Lievens *et al.* (2019), p. 502.
[32] Lamarque (2016), p. 59. Moro lo traduce come "maggiori interessi del bambino": Moro *et al.* (2019), p. 41.
[33] United Nations Committee on the Rights of the Child (2013), p. 9.
[34] Legge 27 maggio 1991, n. 176, "Ratifica ed esecuzione della convenzione sui diritti del fanciullo".
[35] Cfr. Corte cost., sent. 7/2013, in particolare il pt. 6 del "considerato in diritto".
[36] L'art. 6 (3) del Trattato sull'Unione europea prevede che "[i] diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali". Cfr. a riguardo Corte di Giustizia dell'Unione Europea, C-540/03 *Parlamento v. Consiglio* [2006] ECR I-5769, para. 37; Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa (2015), p. 27.
[37] Spiegazione relativa all'articolo 24 — Diritti del minore, Spiegazioni relative alla Carta dei diritti fondamentali, Gazzetta ufficiale dell'Unione europea C 303 del 14 dicembre 2007, pp. 17–35.
[38] Tale principio ha ad esempio conosciuto importante implementazione a livello di normazione e *policy* nell'ambito della giustizia a misura di minore (c.d. *child-friendly justice*). Cfr., per una sintetica panoramica degli elementi da considerare nell'ambito dei procedimenti giudiziali che coinvolgano un minore, Agenzia dell'Unione europea per i diritti fondamentali (2017).
[39] Sull'applicazione della Carta dei diritti fondamentali a livello nazionale si v. Agenzia dell'Unione europea per i diritti fondamentali (2018b).

come si vedrà, non fa eccezione.

4. Il *sexting*: prospettive d'analisi.

La pratica del c.d. *sexting* riunisce in sé una varietà di condotte, tutte caratterizzate dallo scambio tramite le tecnologie informatiche di contenuti di carattere erotico. Un approccio ampio al fenomeno vi fa rientrare sia immagini fotografiche e riprese video, sia messaggi di testo di carattere allusivo. Numerose sono infatti le definizioni che la letteratura giuridica e sociopedagogica ha dedicato a tale fenomeno[40]. La descrizione più ristretta di *sexting* di cui qui si farà uso, tuttavia, lo limita alla produzione, possesso o cessione di immagini o video di carattere pornografico (latamente) autoprodotti[41]. Il concetto di autoproduzione viene qui inteso in un'accezione ampia, che abbraccia – a prescindere dal dato materiale di colui o colei che attiva e tiene fisicamente la fotocamera – sia i materiali prodotti da un minore raffiguranti se stesso, sia quelli da altri prodotti su di lui/lei col relativo consenso. Si pensi al minore che si scatti dei *selfie*, ovvero a quello che consapevolmente si faccia riprendere dal partner, oppure a situazioni ibride dove l'uno attivi la videocamera e l'altro la regga. Come si vedrà nel prosieguo, tale dato materiale ha tuttavia talvolta dato adito a diversi trattamenti penalistici.

Una distinzione va ulteriormente praticata tra *sexting* c.d. "primario" e "secondario". Mentre con il primo termine si indicano quei materiali volontariamente scambiati tra due o più soggetti, con il secondo si fa riferimento all'inoltro non consensuale di tali materiali ad ulteriori persone[42]. Il *sexting* primario ha spesso luogo nell'ambito di una relazione, sebbene questo elemento non sia sempre presente[43]. Rispetto ai casi di pedopornografia come tradizionalmente intesi, il *sexting* inverte il rapporto di offensività tra la condotta primaria (la realizzazione dell'immagine e la sua eventuale volontaria cessione a una persona) e quella secondaria (l'ulteriore diffusione della stessa, contro la volontà del minore). Il danno ai diritti di personalità del minore va infatti ricondotto prevalentemente, se non unicamente, a quest'ultima condotta. Per esemplificare la situazione, si pensi al minore che invii una propria foto intima al partner, e questi – dopo la fine della relazione – la condivida con vari comuni amici.

Pur non essendo di per sé una pratica confinata ai minori di età, il presente contributo si limiterà a trattare di questi ultimi; con l'avvertenza, tuttavia, che pure i fenomeni di *sexting* secondario tra adulti (c.d. *revenge porn*, sebbene tale termine si presenti inesatto)[44] necessitano di adeguata repressione penale, al cui difetto ha pure voluto sopperire l'introduzione dell'art. 612-ter c.p.

Difficile risulta determinare l'effettiva ricorrenza del *sexting* tra minori; gli studi empirici effettuati conducono infatti a risultanze parzialmente contrastanti o eccessivamente vaghe[45]. Ciò consegue sia all'ampiezza di definizioni, che rende i dati tra loro difficilmente comparabili, sia alla relativa "novità" della pratica, sia alla notevolissima sensibilità del tema. Pare infatti lecito chiedersi se i dati che taluni studi riportano non risentano della delicatezza propria dell'argomento, in particolare se raccolti nell'ambito di *focus group* e interviste faccia a faccia con minori, di conseguenza potenzialmente sottostimando l'effettiva incidenza di tali pratiche. Pare tuttavia di poter affermare che non si tratti affatto di un fenomeno marginale[46]. Il titolo

[40] Cfr. Lenhart (2009); Sacco *et al.* (2010); Ringrose *et al.* (2012); Lievens (2014a), p. 254.
[41] Salvadori (2017), p. 793.
[42] Cfr., tra i vari, Villacampa (2017), p. 10.
[43] Già nel 2009, alcuni *focus group* sul tema organizzati negli Stati Uniti rilevavano come lo scambio di immagini possa avvenire anche al di fuori di una relazione sentimentale, ad esempio nei confronti di soggetti con i quali si auspica di sviluppare una maggiore intimità: Lenhart (2009), p. 2
[44] La distribuzione secondaria e non consensuale dei materiali pornografici, c.d. *revenge pornography*, può infatti avvenire a prescindere da una volontà di vendetta (*revenge*). In aggiunta, il termine "*porn*", generalmente connotato negativamente, può essere fonte di ulteriore vittimizzazione della persona da cui tali materiali intimi provengano, ponendo esso in ulteriore, cattiva luce la persona già gravemente lesa dalla diffusione delle immagini. Vari ordinamenti esteri che hanno approntato una risposta normativa a tali pratiche hanno pertanto optato per una diversa definizione delle stesse. Cfr. Caletti (2018a), p. 72.
[45] Cfr. Salvadori (2017), pp. 793–795; si vedano anche gli studi citati da Lievens (2014a), p. 253; Caletti (2018a), p. 76; Stanley *et al.* (2018), p. 2932. Anche con riguardo a fenomeni di estorsione e coercizione sessuale *online* di minori, nel cui ambito il *sexting* può essere fatto rientrare qualora il consenso iniziale sia estorto o carpito maliziosamente, l'Europol rinviene una grave mancanza di studi, in particolare di carattere giuridico-comparato, e richiede che la ricerca accademica vi conceda maggiore attenzione; stesso dicasi per l'uso sessualizzato delle risorse tecnologiche da parte dei minori di età: Europol (2017), pp. 7-10 e 20. Sul tema si v. Salvadori (2018) e Schiavon (2017).
[46] In tal senso Symons *et al.* (2018), p. 3837. Per quanto concerne l'Italia, uno studio effettuato nel 2012 da Telefono azzurro ed Eurispes rilevava come il 25,9% degli adolescenti italiani dai 12 ai 18 anni intervistati avesse ricevuto sms, mms o video di natura sessuale (un

del presente contributo, "send nudes", fa riferimento a una ricorrente espressione per chiedere scatti intimi[47].

Tre ulteriori prospettive sono da considerarsi con riguardo all'incidenza del *sexting* nella società.

Da una parte, l'effettiva carica lesiva di una diffusione non consensuale di materiali intimi autoprodotti può in parte dipendere dal genere della vittima[48]. In società più tradizionali o religiose, una ragazza risente infatti più facilmente di un maggiore danno alla propria reputazione rispetto ai suoi coetanei maschi. Alcune indagini qualitative hanno confermato l'esistenza di tali "doppi standard" anche tra i minori[49].

Allo stesso tempo, il fenomeno dell'*online dating* (dicasi, in generale, la conoscenza di potenziali partner romantici tramite strumenti digitali, pratica in cui può inserirsi il *sexting*) appare più diffuso in contesti minoritari, quali quello LGBTI (lesbiche-gay-bisessuali-transgender-intersex) o quello degli eterosessuali sopra una certa età[50]. In particolare per giovani non-eterosessuali, un forte incoraggiamento a esplorare la propria sessualità *online* può infatti risultare dallo stigma e dalla discriminazione che essi non raramente ancora incontrano nel mondo *offline*[51].

In ultimo, si noti come la letteratura scientifica sempre più valuti il *sexting* in termini di normalità, considerandolo, entro determinati termini, come una legittima componente della propria vita sessuale[52]. Con il diffondersi delle tecnologie, pure la sperimentazione sessuale sarebbe infatti migrata verso tali contesti,[53] sicché essi rileverebbero a livello di diritti fondamentali, in particolare quelli relativi a libera espressione, sviluppo della personalità e privacy[54]. Con riguardo alla percezione che di tale fenomeno hanno i diretti interessati, vari studi ne sottolineano l'elemento ludico e sperimentale[55]. Non da tacere è tuttavia la pressione sociale che non pochi minori avvertono nei confronti delle richieste dei loro coetanei volte a scambiarsi foto intime; pressione a cui soprattutto le ragazze si troverebbero esposte[56]. L'allarme sociale – se non panico[57] – che il *sexting* negli ultimi anni ha causato nel dibattito pubblico, tuttavia, non si riflette necessariamente in positivo sulla prevenzione dei rischi connessi a tale pratica. Non infondata appare infatti la possibilità che tali allarmi incoraggino le istanze pubbliche a "fare qualcosa" per dare risposta alle aspettative sociali, piuttosto che considerare con attenzione le diverse esigenze e situazioni che si celano dietro tale fenomeno[58].

In tal senso, voci autorevoli hanno evidenziato come una politica repressiva, che si limiti a invitare ad astenersi da certe pratiche, non necessariamente si rifletterebbe in una effettiva riduzione dei rischi[59]. Lo Stato dovrebbe pertanto dar seguito ai propri obblighi di tutela con altre e più adeguate modalità, in particolare consolidando nei giovani, per il tramite dei

notevole incremento rispetto al 10,8% dell'anno precedente); si noti tuttavia l'ampia definizione, che non richiede che tali materiali siano effettivamente autoprodotti. A sua volta, il 12,3% degli adolescenti aveva dichiarato di aver inviato materiali a sfondo sessuale: Telefono azzurro ed Eurispes (2012), p. 18 e *passim*. Un'indagine del 2018 ha invece rilevato che il 7% dei ragazzi di 11-16 anni intervistati avrebbe ricevuto "immagini o messaggi di carattere sessuale": Mascheroni e Ólafsson (2018), p. 36.

[47] Si permetta di rinviare alla definizione fornita a proposito da Urban Dictionary.

[48] Lievens (2014a), p. 254, invita ad evitare tale termine, "vittima", per definire la persona danneggiata dal *sexting* o bullizzata, preferendo a tal fine il più neutro "target".

[49] Uno studio internazionale cita ad esempio un ragazzo italiano (Carlo, 17 anni) intervistato durante un'indagine qualitativa: "Se una foto nuda di me dovesse andare in giro per il web, no problem… per una ragazza è diverso… la sua reputazione sarebbe in pericolo…" (traduzione dell'autore dall'articolo inglese): Stanley et al. (2018), p. 2935. Parlano di un "doppio standard" Symons *et al.* (2018), p. 3850.

[50] Rosenfeld e Thomas (2012), p. 540.

[51] Symons *et al.* (2018), p. 3852, con ulteriori riferimenti; gli autori evidenziano al contempo come sia difficile considerare tale variabile negli studi empirici, data la sensibilità del tema. Si v. anche la panoramica di scritti scientifici pubblicati tra il 2009 e il 2013 proposta da Döring (2014). Sul tema cfr. Noto La Diega (2019) e Zalnieriute (2019).

[52] Symons *et al.* (2018), p. 3837; Bulger *et al.* (2017); Shariff (2015), p. 77; Lievens (2014a), p. 254; Villacampa nota tuttavia come gli studi che riconducano il *sexting* alla normalità siano più diffusi in Europa rispetto agli Stati Uniti: Villacampa (2017), 12 e 18.

[53] Shariff (2015), p. 77; Bulger *et al.* (2017), p. 759.

[54] Shariff (2015), p. 77; Bulger *et al.* (2017), p. 759. Segue tale impostazione, riconducendo il *sexting* alla libertà di espressione e privacy così come riconosciute ai minori dalla Convenzione ONU anche ai fini dell'esplorazione della propria sessualità, Lievens (2014a), p. 268. In tal senso pure l'autorevole opinione di Tobin e Parkes (2019), p. 449.

[55] Stanley *et al.* (2018), p. 2934 s., che riferiscono come molti dei ragazzi intervistati nel corso dell'indagine qualitativa considerino il *sexting* come un fenomeno normale.

[56] Gli stessi ricercatori rilevano come tale pratica, sebbene percepita come normale, riproduca stereotipi sessisti: Stanley *et al.* (2018), p. 2920; cfr. anche Shariff (2015), p. 69, e Lenhart (2009), p. 8.

[57] Parlano di "*moral panic*" sia Villacampa (2017), p. 11, sia Lievens (2014a), p. 253.

[58] Bulger *et al.* (2017), pp. 752 e 753.

[59] Ad esempio, è stato osservato come le politiche di educazione sessuale diffuse negli Stati Uniti basate sull'astinenza sessuale abbiano fatto diventare internet la fonte primaria di informazioni a proposito, uno sviluppo non necessariamente positivo: Stanley *et al.* (2018), p. 2921. Critico nei confronti di tali politiche anche Döring (2014).

canali educativi formali e informali, quelle competenze di carattere emozionale e psicosociale per decidere se, con chi, entro quali limiti e in che modo, (non) scambiare proprie immagini intime con soggetti loro vicini[60].

5. L'evoluzione normativa delle fattispecie di pornografia minorile.

5.1. *Breve cronistoria degli sviluppi normativi, fortemente influenzati dalle fonti europee ed internazionali.*

Come noto, il reato di pornografia minorile è previsto dall'art. 600-ter c.p., ove venne introdotto nel 1998[61]. La definizione legale, aggiunta nel 2012[62], intende con tale termine "ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali". La disposizione punisce oggi al comma primo chiunque "utilizzando minori di anni diciotto, […] produce materiale pornografico". I commi terzo e quarto puniscono rispettivamente chi "distribuisce, divulga, diffonde o pubblicizza" ovvero "offre o cede ad altri, anche a titolo gratuito" il materiale pornografico "di cui al primo comma". Il bene giuridico è stato inizialmente individuato nella libertà individuale nella sua accezione più ampia, sebbene sia stato presto osservato come il reato di pornografia minorile sia plurioffensivo, andando in particolare a interessare anche il libero sviluppo personale del minore[63]. Al contempo, l'art. 600-quater punisce, quale norma di chiusura, la detenzione di pornografia minorile, punendo chi, al di fuori delle ipotesi previste dalla disposizione precedente, consapevolmente si procuri o detenga materiale pornografico realizzato utilizzando minori.

Al momento della sua introduzione nel 1998, l'art. 600-ter richiedeva al comma primo lo "sfruttamento" del minore quale requisito della condotta. Una certa linea interpretativa lesse tale requisito quale richiedente l'uso del minore con finalità lucrative o commerciali, o comunque con ricadute economiche[64]. In senso contrario si espressero tuttavia le Sezioni Unite già nel 2000[65], delimitando al contempo l'applicazione dell'articolo in questione ai casi in cui potesse desumersi un pericolo concreto di diffusione del materiale. Il legislatore, nel 2006[66], ha quindi fatto propria l'ampia lettura dello "sfruttamento" del minore, sostituendo tale potenzialmente equivoco termine con il più generico "utilizzazione", senza invece esprimersi sul pericolo di diffusione. Su tale ultimo punto è infine intervenuta nel 2018 una decisione delle Sezioni Unite, ritenendo – tra le altre cose[67] – non più attuale il requisito della pericolosità concreta di diffusione al fine dell'integrazione della fattispecie[68].

Ulteriori modifiche[69] alla disciplina sono intervenute nel 2006 e nel 2012, mentre il capo

[60] Fra i vari, Lievens (2014a), p. 268; Döring (2014).
[61] Legge 3 agosto 1998, n. 269 "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù".
[62] Legge 1 ottobre 2012, n. 172 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale, fatta a Lanzarote il 25 ottobre 2007, nonché norme di adeguamento dell'ordinamento interno".
[63] In tale ultimo senso Cass. pen. (SS. UU.) 13/2000; Mantovani (2016), pp. 462 ss. Sulle varie linee dottrinali a riguardo, con ulteriori riferimenti, Pistorelli (2015), pp. 224 ss. Sul reato di pedopornografia la letteratura è sterminata; tra i vari, Picotti (2007), Bertolino (2010), Helfer (2007 e 2012) e, più recentemente, i vari contributi sul tema in Cadoppi *et al.* (2019).
[64] Per riferimenti dottrinali con riguardo ai sostenitori della tesi economicistica e della tesi non economicistica si v. Mantovani (2016), p. 503.
[65] Cass. pen. (SS. UU.) 13/2000. La Corte ha in tale contesto affermato che il termine "sfruttare" andava letto in termini ampi, comprendenti pure quelle condotte non finalizzate a ottenere, dalla realizzazione dei materiali pedopornografici, vantaggi di carattere economico.
[66] Legge 6 febbraio 2006, n. 38 "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet".
[67] Per una più completa analisi della sentenza si v. *infra* nel testo.
[68] Anche alla luce delle riforme che a partire dal 2006 hanno interessato la fattispecie e delle fonti di diritto internazionale ed europeo che le stesse hanno ispirato (si v. subito *infra* nel corpo dell'articolo), la disposizione non sarebbe da leggersi (più) come richiedente un pericolo concreto di diffusione del materiale pornografico. Tali innovazioni normative miravano infatti a offrire al minore una più ampia tutela della sua immagine, dignità e corretto sviluppo sessuale; beni giuridici, questi, compromessi già al momento della realizzazione del materiale pornografico, a prescindere dalla sua successiva divulgazione. In aggiunta, il profondo mutamento tecnologico avrebbe reso la richiesta prova del concreto rischio di diffusione del tutto "anacronistica", essendo questo insito nella connettività a internet oggigiorno generalmente diffusa. Diversa era la situazione che si presentava nel 2000, dove un tale accesso costituiva un *quid pluris* da accertarsi di volta in volta. Giustamente è tuttavia stato osservato come una tale considerazione riproponga in forma surrettizia il requisito del pericolo concreto, sebbene questi risulti oggi implicito: Bertolesi (2018), pt. 7.
[69] Una breve sintesi degli interventi normativi che hanno interessato tale disposizione si rinviene in Pistorelli (2015), pp. 229 ss.

del codice in cui essa è inserita, "Dei delitti contro la libertà individuale", per quanto qui di rilievo è stato innovato in ultimo nel 2014[70]. Tali innovazioni legislative conseguono al recepimento di quattro importanti atti di diritto internazionale ed europeo, dicasi il protocollo opzionale alla Convenzione ONU concernente la vendita, la prostituzione e la pornografia rappresentante bambini, adottato nel 2000; la decisione quadro 2004/68/GAI del Consiglio dell'Unione europea volta alla lotta contro lo sfruttamento sessuale dei bambini e contro la pornografia infantile (d'ora innanzi: la decisione quadro); la Convenzione del 2007 del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale (in seguito: la Convenzione di Lanzarote)[71]; e la direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile (brevemente: la direttiva)[72].

5.2. *Il mancato uso da parte del legislatore italiano della clausola di non punibilità per il* sexting *consensuale.*

Tali ultimi tre atti di diritto internazionale ed europeo, che hanno ispirato e in misura consistente plasmato la disciplina italiana, nell'imporre la severa repressione delle condotte di pornografia minorile, autorizzano gli Stati a non perseguire lo scambio di immagini di contenuto pornografico liberamente realizzate da un minore e da questi condivise con altri. La decisione quadro prevede così la possibilità di non reprimere la produzione e il possesso di "immagini di bambini che abbiano raggiunto l'età del consenso sessuale e siano prodotte e detenute con il loro consenso e unicamente a *loro* uso privato (art. 3 (2) let. b) della decisione quadro). Stesso dicasi per la Convenzione di Lanzarote nel caso di "materiale pornografico che coinvolge minori che abbiano raggiunto l'età [del consenso sessuale][73], quando tali immagini sono prodotte o possedute *dagli stessi*, con il loro consenso ed esclusivamente per *loro* uso privato" (art. 20, para. 3 della Convenzione di Lanzarote)[74]. Al contempo, la direttiva all'art. 8 (3) fa rientrare nella discrezionalità degli Stati membri la decisione se reprimere la "produzione, [l'] acquisto o [i]l possesso di materiale pedopornografico in cui sono coinvolti minori che abbiano raggiunto l'età del consenso sessuale nei casi in cui tale materiale è prodotto e posseduto con il consenso di tali minori e unicamente a uso privato *delle persone coinvolte*, purché l'atto non implichi alcun abuso" (enfasi aggiunta).

La clausola della direttiva pare di più ampia applicazione rispetto alle corrispondenti previsioni della decisione quadro e della Convenzione di Lanzarote. Essa infatti non richiede che la produzione o il possesso di materiale pornografico ritraente i minori sia rivolto unicamente all'uso privato da parte di questi. Al contrario, è richiesto che esso sia prodotto consensualmente e posseduto a uso privato "delle persone coinvolte". L'uso di tale espressione appare frutto di una scelta consapevole, sia alla luce della diversa formulazione impiegata nella decisione quadro che la direttiva va a sostituire, sia dei termini utilizzati nei restanti paragrafi dell'art. 8[75]. Allo stesso tempo, pure il considerando n. 20 della direttiva chiarisce come essa non intenda disciplinare le politiche degli Stati membri "in ordine agli atti sessuali consensuali che possono compiere i minori e che possono essere considerati come la normale scoperta della sessualità legata allo sviluppo della persona, tenendo conto delle diverse tradizioni culturali e giuridiche *e delle nuove forme con cui bambini e adolescenti stabiliscono e mantengono rapporti tra di loro, anche a mezzo di tecnologie dell'informazione e della comunicazione*" (enfasi aggiunta).

Pare conseguentemente un'interpretazione fedele al dato letterale e sistematico fare rientrare nelle "persone coinvolte" di cui all'art. 8 (3) della direttiva anche i maggiore di età, fatto

[70] D. lgs. 4 marzo 2014, n. 39 "Attuazione della direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che sostituisce la decisione quadro 2004/68/GAI".

[71] Già la Convenzione del Consiglio d'Europea sul cybercrime, data a Budapest nel 2001, richiedeva la repressione dei reati correlati alla pornografia minorile (art. 9); l'art. 20 della Convenzione di Lanzarote si è ispirato proprio alla Convenzione di Budapest: Consiglio d'Europa (2007), p. 20.

[72] Si noti che la direttiva viene talvolta erroneamente indicata quale "2011/92/UE", in conseguenza di una sbagliata denominazione avvenuta al momento della pubblicazione.

[73] Per una ricerca comparatistica sull'età del consenso sessuale nei Paesi membri dell'UE si v. Agenzia dell'Unione europea per i diritti fondamentali (2018a). Si noti come sia la Convenzione di Lanzarote, sia la direttiva specifichino chiaramente come esse non siano volte all'armonizzazione dell'età del consenso sessuale (art. 2 della direttiva; art. 18 para. 2 della Convenzione di Lanzarote).

[74] Convenzione di Lanzarote, così come tradotta nella legge di ratifica 1 ottobre 2012, n. 172.

[75] In essi la direttiva attribuisce alla discrezionalità degli Stati membri la decisione se reprimere gli atti sessuali e gli spettacoli pornografici tra "coetanei, vicini per età, grado di sviluppo o maturità psicologica e fisica".

salvo il rispetto degli ulteriori criteri enunciati dalla disposizione. Seguendo tale linea interpretativa, anche l'adulto che realizzi del materiale pedopornografico con il consenso del minore andrà così immune da pena, qualora esso sia prodotto unicamente a loro uso privato e l'atto non implichi alcun abuso. Si pensi, ad esempio, a una coppia dove un partner sia diciottenne e l'altro minore di età, e il primo scatti delle foto intime al secondo, con il consenso libero di questi, volendo mantenere riservate le immagini realizzate. Si noti tuttavia che la clausola estende la sua efficacia soltanto alla produzione, acquisto e possesso del materiale pornografico (di cui all'art. 5, paragrafi 2 e 6, a cui fa riferimento); non, invece, alla distribuzione, diffusione o trasmissione dello stesso (di cui all'art. 5, paragrafo 4, della direttiva). Per tornare all'esempio, la condotta del partner (diciottenne o meno) che diffonda ulteriormente le immagini del minore non rientrerebbe pertanto nell'ambito applicativo della clausola.

L'Italia, tuttavia, non ha mai fatto uso di alcuna di tali possibilità di scriminare le condotte, oggettivamente pedopornografiche, realizzate in maniera libera e consensuale. L'ordinamento nazionale non differenzia, rispetto alla fattispecie generale, la produzione e il possesso di materiale pedopornografico consensualmente prodotto. Nel corso dei lavori preparatori della legge n. 38/2006 di riforma delle fattispecie di pedopornografia in luce della decisione quadro, il Governo aveva sì proposto l'introduzione di specifiche cause di non punibilità; queste, tuttavia, non sono state riprodotte nella versione finale del testo normativo[76]. Varie voci in dottrina hanno conseguentemente osservato come tale scelta consapevole del legislatore non possa che attribuire rilevanza penale alle condotte di c.d. "pornografia domestica" minorile[77]. A fondamento di tale trattamento unitario è stata ripetutamente avanzata la necessità di reprimere a monte la creazione di materiale pornografico ritraente minori, la cui diffusione potrebbe alimentare il circuito della pedopornografia[78].

6. Valutazione giurisprudenziale del *sexting*.

6.1. *Primi orientamenti delle Corti di legittimità e merito.*

In linea con il quadro normativo delineato, la giurisprudenza italiana ha generalmente ricondotto le condotte di *sexting* alle fattispecie di pornografia minorile[79]. In questione sono venuti pertanto l'art. 600-ter, seppure l'applicazione era limitata dalla tradizionale interpretazione che richiedeva per la sua configurabilità il pericolo concreto di diffusione dei materiali, e l'art. 600-quater.

Per concentrare questa panoramica in particolare sulle decisioni di legittimità, non sorprenderà che la Cassazione ha cominciato ad occuparsi del tema in tempi abbastanza recenti. I telefoni che permettono di realizzare e inviare delle immagini, e successivamente gli *smartphone*, si sono infatti diffusi nel nostro Paese in anni non molto distanti. A chi scrive risulta che la Corte abbia avuto modo di esprimersi una prima volta sul tema con la sentenza n. 27252 del 2007, inerente a delle misure cautelari applicate a un minore con riguardo alla fattispecie di cui all'art. 600-ter c.p. Il caso in cui esse si inserivano concerneva la trasmissione su più telefoni di una ripresa ritraente un rapporto sessuale tra una minore tredicenne e un'altra persona, all'interno di un quadro più ampio caratterizzato da abusi e costrizioni. Nell'analisi della legittimità dell'applicazione delle misure, il collegio incidentalmente rileva come la previsione normativa di cui al 600-ter intenda offrire ai minori una tutela anticipata avverso azioni "di per sé degradanti e connotate da profondo disvalore, oltre che pericolose per la successiva eventuale diffusione che il materiale così prodotto o raccolto può conoscere". A riguardo, i giudici danno valore al fatto che il legislatore mai avrebbe attribuito rilievo alcuno al consenso eventualmente prestato alla realizzazione delle immagini pornografiche. Mentre

[76] Cfr. art. 3 d.d.l. n. 4599, XIV legislatura: "Dopo l'articolo 600-quater del codice penale […] sono inseriti i seguenti […] Art. 600-quater. 3. (Altri casi di non punibilità). Non è punibile chi produce il materiale pornografico di cui agli articoli 600 ter, primo comma, e 600-quater.1, primo comma, quando il materiale è prodotto e detenuto da minore degli anni diciotto e ritrae o rappresenta un minore che abbia raggiunto l'età del consenso sessuale, e sia rimasto nell'esclusiva disponibilità dei soli soggetti minori rappresentati".
[77] Fra i vari: Ferla (2017), p. 1962; Bianchi (2016), p. 146; nota che il mancato uso delle forme di esclusione della responsabilità in tali circostanze è avvenuto "forse inopportunamente" Delsignore (2015), p. 741.
[78] In tal senso si può richiamare già Cass. pen. (SS. UU.) 13/2000, pt. 5.2.
[79] Riepiloga gli sviluppi giurisprudenziali Cass. pen. (SS. UU.) 51815/2018, pt. 4.1.2 del "considerato in diritto".

i rapporti sessuali rappresentano infatti "una fisiologica espressione della personalità […] del tutto diversa è la situazione in caso di condotte che presuppongono sia una offesa alla dignità del minore coinvolto in realizzazione pornografiche sia una evidente sproporzione nella posizione di forza dei soggetti coinvolti".

La Cassazione ripete una similare linea argomentativa nel 2012 tramite la sentenza n. 47239, concernente il video di un rapporto sessuale tra due minorenni, registrato consensualmente e quindi diffuso illegittimamente da uno dei due. Il collegio ripropone il distinguo valoriale tra rapporti sessuali e la realizzazione di materiali pornografici, rilevando come non si possa ritenere scriminante "l'eventuale consenso del minore al fatto [la realizzazione degli scatti intimi, n.d.a.], considerato che esso proverrebbe da persona immatura, che non ha la disponibilità di diritti inalienabili, quali la libertà psicofisica"[80].

Ulteriori sentenze di legittimità vengono non raramente menzionate per sostenere l'irrilevanza del consenso del minore alla realizzazione di materiali di carattere pornografico[81]. Esse tuttavia presentano costellazioni fattuali caratterizzate da episodi di costrizione e/o abuso già al momento della registrazione dei filmati o delle fotografie, con la conseguenza che l'eventuale consenso risulta non libero e pertanto in ogni caso non rilevante[82].

Una decisa svolta nel senso del riconoscimento del valore del consenso del minore si rinviene invece in una sentenza della Corte d'appello di Milano del 2014[83], in conferma di una sentenza del Tribunale meneghino. Un ventenne e una quindicenne si erano scambiati varie proprie foto nude, senza che queste trovassero ulteriore diffusione; a seguito della denuncia dei genitori di lei, si era giunti a processo. Sì da determinare se la minore fosse stata "utilizzata" per la realizzazione di tale materiale, come richiesto dal reato di detenzione di materiale pedopornografico *ex* art. 600-quater c.p .[84], i giudici rilevano come nel caso di specie non avesse avuto luogo alcuna induzione subdola allo scambio di immagini. Esso si era infatti realizzato in un rapporto a due, in cui entrambi i soggetti avevano conservato le foto che reciprocamente si erano inviati. I giudici si dedicano pertanto alla delimitazione delle condizioni in presenza delle quali attribuire rilevanza al consenso e osservano come questi vada considerato alla luce delle circostanze complessive in cui si esplica. Rilevano in particolare l'età del minore, le modalità della richiesta e della sua espressione, il coinvolgimento o meno di terzi e la destinazione successiva delle immagini. Alla luce di ciò e dei principi di tassatività e offensività, la Corte ritiene che reputare illecita la condotta in oggetto reprimerebbe delle condotte "che il sistema complessivo delle norme penali ha viceversa inteso far rientrare nella sfera delle libertà individuali, di cui, evidentemente, sono portatori anche i minori". A riprova che "la tutela dei minori non elida la loro capacità di autodeterminazione" la Corte cita varie norme, penali e civili, che attribuiscono rilevanza all'opinione del minore[85]. La sentenza di piena assoluzione dell'imputato trova così conferma.

[80] In aggiunta, la Corte torna a ripetere che ogni rilevanza del consenso sarebbe stata implicitamente rigettata dal legislatore, che non ha recepito le cause di non punibilità prospettate durante i lavori parlamentari che hanno portato alla legge n. 38/2006. La Corte conferma quindi la condanna inflitta al minore colpevole della diffusione del filmato in ordine ai reati di cui all'art. 600-ter c.p., quarto comma, per aver ceduto materiale pornografico realizzato utilizzando una minore, e 595 c.p., diffamazione, per aver offeso la reputazione di quest'ultima.

[81] Si v. ad esempio le prospettazioni della Procura Generale così come riassunte, e respinte, dalla Corte d'appello di Milano, ud. 12 marzo 2014, Pres. Rizzi, Est. Domanico, in *penalecontemporaneo.it*, 17 giugno 2014, con nota di Sassaroli. Sulla sentenza meneghina si v. subito *infra* nel corpo dell'articolo.

[82] Si v. Cass. pen. 43414/2010, inerente a materiali realizzati nell'ambito di rapporti con una ragazza avviata alla prostituzione e sfociati anche in condotte di violenza sessuale; Cass. pen. 1181/2011, dove l'imputato era stato rinvenuto in possesso di un CD con immagini pedopornografiche raffiguranti numerosi minori, del cui contenuto si era dichiarato non consapevole; Cass. pen. 11997/2011, che tratta di un filmato realizzato all'insaputa di due soggetti minori; Cass. pen. 39872/2013, dove l'imputato aveva adescato una minore con la prospettazione ingannatoria di dover realizzare un catalogo di costumi da bagno; Cass. pen. 41776/2013, in cui un adulto aveva chiesto a una minore undicenne di mostrarsi nuda al computer in quanto "anche altre [minori] lo fanno"; Cass. pen. 39039/2018, dove il materiale autoprodotto era stato inviato con minaccia di percosse. La sentenza n. 6119/2016 si limita invece ad esaminare la liquidazione del danno riconosciuta alle parti civili, dicasi una minore che aveva realizzato un video pornografico, inviato all'imputato e da questi diffuso. Evidenziando il ruolo attivo della parte offesa – che si sarebbe volontariamente o comunque consapevolmente esposta al rischio di vedere il video diffuso –, i supremi giudici ritengono appropriato il limitato risarcimento riconosciuto in appello. Non oggetto di gravame era invece la riconduzione della condotta alla fattispecie di cui all'art. 600-ter c.p., così come operata in secondo grado.

[83] Corte d'appello di Milano, ud. 12 marzo 2014, cit.

[84] L'imputazione ex art. 600-ter c.p. era infatti venuta meno in considerazione del fatto che la disposizione richiedeva un pericolo concreto di diffusione del materiale; diffusione che, dati i rapporti tra i due giovani, non si era avuta né era da attendersi nel caso portato all'attenzione dei giudici.

[85] Si v. ad esempio le innovazioni apportate al diritto di famiglia dalla legge 10 dicembre 2012, n. 219, e dal d. lgs. 28 dicembre 2013, n. 154. Rispetto all'impostazione tradizionale del codice civile, impregnato di una logica patrimoniale, in particolare le riforme dell'ultimo quinquennio hanno definitivamente affermato il riconoscimento del minore quale persona titolare di diritti autonomi: lo ricorda, in ultimo, Pisu (2019), p. 2.

Parzialmente diverso ma comunque importante, nel senso di attribuire rilevanza giuridica al consenso del minore alla realizzazione dei materiali, un caso deciso dal Tribunale di Firenze nel 2015[86]. Un video di una minore, registrato consensualmente dall'allora partner maggiorenne, era stato diffuso da questi dopo la rottura del rapporto sentimentale. Anche qui i giudici escludono la rilevanza dell'art. 600-ter, primo comma, proprio alla luce del consenso espresso dalla minore. La realizzazione dei filmati era infatti avvenuta su libera iniziativa della minore stessa, facendo venire meno il requisito dell'"utilizzazione". Tale criterio, infatti, va valutato "tenendo conto anche del possibile consenso prestato dal minore", qualora "vi sia stata una facoltà effettiva di scelta ed una decisione consapevole". Il giudice ritiene tuttavia l'imputato colpevole del reato di diffusione di pornografia minorile *ex* 600-ter c.p., terzo comma, per aver diffuso il filmato contro la volontà della minore. Tale capoverso non richiederebbe infatti di indagare "se il minore abbia prestato il suo consenso o se, comunque, il minore sia stato 'utilizzato'". Trattasi tuttavia di una lettura lontana dal dato testuale. Pur comprensibile nel tentativo di reprimere condotte – quelle di diffusione non consensuale di filmati intimi – latrici di notevolissimi danni personali e sociali per il minore, tale interpretazione non risulta sostenibile alla luce della lettera della disposizione. L'art. 600-ter, comma terzo, richiede infatti esplicitamente che il materiale prodotto sia quello "di cui al primo comma", la cui produzione deve essere caratterizzata dall'utilizzazione del minore[87].

Su tale duplice ordine di aspetti – il rilievo del consenso ai fini della determinazione dell'"utilizzazione" e i richiami interni all'art. 600-ter – è tornata ad esprimersi, nel 2016, la Cassazione. Nella sentenza n. 11675 si dibatteva di alcune fotografie scattatesi da una minore e da questa inviate a un certo numero di conoscenti minorenni, che a loro volta, senza consenso, le avevano inoltrate a propri contatti. Ai minori era stato contestato il reato di pornografia minorile ex art. 600-ter comma terzo[88], per aver distribuito, divulgato e diffuso il materiale. Il Tribunale per i minorenni de L'Aquila li aveva assolti, in considerazione del fatto che la produzione originaria delle immagini era avvenuta in maniera volontaria da parte della minore stessa, difettando così la necessaria alterità e diversità dell'autore della condotta rispetto al minore sfruttato. La Cassazione condivide tale lettura, notando come tali due requisiti siano presupposti logici, ancor prima che giuridici, di una "utilizzazione" comunque intesa. Qualora il materiale sia stato prodotto dal minore in modo "autonomo, consapevole, non indotto o costretto", non sarebbe possibile rinvenire utilizzazione alcuna dello stesso. Il consenso che il minore stesso abbia eventualmente prestato alla realizzazione dei materiali pornografici si presenterebbero invece quale "del tutto irrilevante". Qualora al momento della condotta originaria non si rinvenga utilizzazione del minore, a cascata neanche i commi successivi potrebbero venire in questione, facendo questi indissolubilmente riferimento al primo, a pena di un'analogia *in malam partem*.

Tale ultima interpretazione dei richiami interni all'art. 600-ter c.p. pare condivisibile e fedele al dato testuale[89]. Ciononostante, risulta evidente come una tale soluzione, impeccabile sul piano del diritto positivo, abbia come conseguenza un macroscopico vuoto di tutela nei confronti di condotte perniciosissime e di dirompente effetto lesivo: quelle di coloro che, ricevuta un'immagine pornografica realizzata volontariamente, la diffondono senza consenso. Tale vuoto di tutela risulta ulteriormente grave in considerazione del dato empirico che parte consistente delle immagini illecitamente inoltrate e diffuse sarebbero, originariamente, proprio scatti auto-prodotti[90].

Criticabile è invece la lettura dell'"utilizzazione" del minore in termini di mera alterità e diversità dell'autore della condotta rispetto al minore ritratto. Tre sono infatti gli scenari che si possono presentare in occasione della produzione consensuale dei materiali intimi. Questi possono venire realizzati autonomamente dal minore; oppure venire prodotti da un partner o conoscente del minore, col consenso di questi (il materiale si presenterebbe così "eteroprodotto"); ovvero, ed è la terza ipotesi, venire realizzati parzialmente e dall'uno e dall'altro

[86] Tribunale di Firenze, GIP, 10 febbraio 2015, n. 163, in *penalecontemporaneo.it*, 22 aprile 2015, annotata da Verza (2015).
[87] Stesso dicasi con riguardo all'art. 600-quater, non applicato dal giudice fiorentino in quanto norma di chiusura. La Cassazione ha a proposito più volte ricordato come pure tale disposizione richieda l'utilizzazione del minore, non potendo condurre la considerazione come all'art. 600-quater il legislatore abbia optato per una indicazione estesa senza rinviare sinteticamente all'art. 600-ter, comma primo, a conclusioni interpretative difformi rispetto all'art. 600-ter c.p.: Cass. pen. 11675/2016, pt. 9 del "considerato in diritto".
[88] All'unico minore che non aveva inoltrato le immagini era stato contestato il reato di detenzione di pornografia minorile ex 600-quater; assolto in merito, la sua posizione non era stata oggetto di gravame da parte della Procura generale.
[89] Si v. ad esempio la decisione del Tribunale di Firenze e Cass. pen. 47239/2007, *supra*.
[90] Caletti sostiene che l'80% dei casi di divulgazione originerebbe in immagini auto-scattate: Caletti (2018a), p. 86.

scambiandosi la fotocamera, ad esempio nel caso di un filmato. Ci si potrebbe chiedere quale sia il discrimine in proposito, qualora il criterio sia da rinvenirsi nell'alterità e nella diversità del soggetto autore rispetto al soggetto ritratto: colui che attiva la videocamera? Colui che la sorregge fisicamente? Cosa succederebbe qualora i due si alternassero nell'uso della stessa? Una linea di distinzione basata su tali elementi pare poco ragionevole[91].

6.2. *Gli sviluppi giurisprudenziali dalla fine del 2018 avverso la criminalizzazione della "pornografia domestica" compiuta da minori.*

Sull'interpretazione dell'art. 600-ter c.p. sono tornate ad esprimersi, nel 2018, le Sezioni Unite con la sentenza n. 51815[92]. La questione posta all'attenzione della Cassazione – inizialmente della terza sezione, quindi innanzi al suo più autorevole consesso – era se, per l'integrazione dell'art. 600-ter, comma primo, fosse ancora da richiedersi il pericolo concreto di diffusione delle immagini, così come previsto dalla sentenza n. 13/2000 delle stesse Sezioni Unite. Come visto, la risposta che la Cassazione fornisce, richiamando le varie fonti di diritto internazionale ed europeo che hanno a più riprese plasmato la disciplina italiana sulla pedopornografia, è negativa[93].

Decisa tale questione, il collegio si dedica in un *obiter dictum* alla pornografia domestica compiuta da minori che abbiano raggiunto l'età del consenso sessuale. Le fattispecie di contrasto alla pedopornografia, infatti, mal si rapportano a venire applicate nei confronti di tale fenomeno, anche alla luce della tutela rigorosissima e delle ingenti pene da esse previste. A riguardo i giudici rilevano il rischio di un'applicazione eccessivamente espansiva della norma penale, "ben al di là di ipotesi che rispecchino la gravità sociale e lo spessore criminale del fenomeno della pedopornografia". A proposito vanno infatti evitate "'ipercriminalizzazioni' non coerenti con le finalità proprie del diritto penale"; le severissime sanzioni previste ai fini della repressione della pedopornografia, infatti, "sarebbero ingiustificabili, alla stregua del principio costituzionale di ragionevolezza, qualora si volessero ritenere applicabili al fenomeno della 'pornografia minorile domestica'".

Per scongiurare tale rischio, i giudici invitano a valorizzare il dato dell'appartenenza di tali condotte "all'ambito 'dell'autonomia privata sessuale'", qualora i materiali siano realizzati con il consenso dei minori e unicamente a uso privato delle persone coinvolte. Pur usando una diversa terminologia, i giudici si propongono di tutelare una certa autodeterminazione del minore in riferimento al proprio sviluppo sessuale, che a sua volta inerisce alla tutela dei suoi diritti di personalità e di privacy. A tal fine la Corte invita a valorizzare il concetto di utilizzazione del minore, intendendosi però con tale termine "la trasformazione del minore, da soggetto dotato di libertà e dignità sessuali, in strumento per il soddisfacimento di desideri sessuali di altri o per il conseguimento di utilità di vario genere". In presenza di un tale utilizzo strumentale del minore, il consenso eventualmente da questi prestato risulterebbe invalido. Non è quindi il consenso del minore di per sé a far venire meno l'illiceità della condotta, dovendo esso venire letto in un quadro più ampio che consideri il contesto in cui viene a esistenza. Qualora tuttavia si tenga presente che ogni consenso, per essere valido, debba essere libero, consapevole e informato, non appare ardito considerare unitariamente tali due canoni d'analisi.

Le condotte di utilizzazione sarebbero pertanto quelle riconducibili a una "posizione di supremazia […] o per le modalità con le quali il materiale pornografico viene prodotto (ad esempio, minaccia, violenza, inganno) o per il fine commerciale […] o per l'età dei minori coinvolti, qualora questa sia inferiore a quella del consenso sessuale". Diverso è il caso di un rapporto non condizionato, in cui lo scambio delle immagini o dei video sia frutto di una libera scelta. Il collegio menziona, espressamente in via esemplificativa, una relazione paritaria tra minorenni ultraquattordicenni in cui le riprese siano destinate ad un uso strettamente privato. Rilevando come tale conclusione sia prossima alle circostanze fattuali in cui la normativa internazionale ed europea avrebbe permesso di prevedere normativamente delle forme

[91] In tal senso anche Bianchi (2016), pp. 144, 147 e 153.
[92] Cass. pen. (SS. UU.) 51815/2018, ud. 31 maggio – dep. 15 novembre 2018; per un recente commento si v. Bianchi (2019). Il caso concerneva un ministro di culto che, millantando contatti nel mondo della televisione, aveva realizzato del materiale pornografico con minori affidatigli, inducendoli a partecipare a esibizioni pornografiche.
[93] Si v. *supra* par. 3.

di esclusione della responsabilità, a cui il legislatore italiano non ha dato seguito, i giudici si preoccupano infine di precisare come sia lo stesso concetto normativo di "utilizzazione" ad imporre tale conclusione[94].

7. Le innovazioni del "Codice rosso" per ovviare a un gravissimo vuoto di tutela: primi cenni sul reato di diffusione illecita di immagini o video sessualmente espliciti (612-ter c.p.).

La situazione originatasi a seguito di tale – pur condivisibile – arresto giurisprudenziale si presentava seriamente carente nella repressione di condotte di dirompente carattere lesivo. Venendo meno, alle condizioni indicate dalla Suprema Corte, il carattere di "utilizzazione" del minore al momento della realizzazione consensuale delle immagini, pure l'ulteriore diffusione che di esse illecitamente si dovesse fare rimane infatti fuori dall'ambito applicativo delle fattispecie di pedopornografia. La liceità originaria della produzione del materiale pornografico minorile esplica infatti effetti a cascata. Gli attuali rinvii interni alle disposizioni codicistiche di contrasto alla pedopornografia non permettono – salvo illegittime forzature del testo normativo, correttamente escluse dalla giurisprudenza di legittimità – di reprimere tramite esse la distribuzione che di questi materiali si dovesse fare.

Vero è che altre previsioni normative potrebbero venire invocate; tra le varie, i reati di diffamazione (art. 595 c.p.), atti persecutori (art. 612-bis c.p.), diffusione di riprese e registrazioni fraudolente (617 septies c.p.)[95], estorsione (art. 629 c.p.), illecito trattamento di dati personali (art. 167 codice privacy), ed eventualmente l'accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) qualora i materiali venissero carpiti illegittimamente[96]. Si tratta però di disposizioni previste per tutelare specificamente altri beni giuridici. Conseguentemente, non sempre ricorrono le circostanze richieste per la loro integrazione (ad es., nel caso degli atti persecutori, la reiterazione della condotta ovvero, per la diffamazione, la presenza di più persone). Ancor prima, tali fattispecie inevitabilmente girano attorno al problema che qua interessa, senza coglierne in pieno il carattere offensivo e reprimerlo efficacemente[97].

Di un "vuoto di tutela" parla la stessa Cassazione, non essendo tali fenomeni stati adeguatamente considerati dal legislatore al momento della stesura e riforma delle fattispecie codicistiche[98]. Tale carenza normativa tradisce gli espliciti obiettivi delle leggi di contrasto alla pedopornografia, dicasi la protezione dei minori contro lo sfruttamento e l'abuso sessuale. Ancor prima, tale situazione risulta in grave violazione degli obblighi internazionali ed eurounitari di tutela del minore da ogni forma di violenza, di sfruttamento sessuale e di violenza sessuale[99], scaturenti in particolare dalla Convenzione ONU sui diritti del fanciullo e dei relativi Protocolli, dalla Convenzione di Lanzarote e dalla direttiva 2011/93/UE. Tutti tali atti impongono infatti di dare adeguata repressione alle condotte di diffusione di materiali pedopornografici.

L'ordinamento italiano ha posto parziale rimedio a tale situazione con la recentissima riforma del c.d. "Codice rosso"[100]. La legge, entrata in vigore nell'agosto 2019, si propone di contrastare la violenza domestica e di genere e ha a tal fine modificato in più punti l'ordinamento penale e processualpenale. Per quanto rileva per il tema qui trattato, essa ha introdotto nel titolo XII, capo III, sezione III del codice penale ("Dei delitti contro la libertà morale"), una nuova fattispecie di reato. L'art. 612-ter c.p., rubricato "Diffusione illecita di immagini o video sessualmente espliciti", punisce chiunque, dopo averli realizzati o sottratti, "invia, consegna, cede, pubblica o diffonde" senza consenso immagini o video a contenuto sessualmente esplicito e destinati a rimanere privati. La sanzione consiste nella reclusione da uno a sei anni e nella multa da 5.000 a 15.000 euro.

[94] Una prima applicazione di tale innovativa linea interpretativa si è avuta, poche settimane dopo il suo deposito, tramite la sentenza n. 55000/2018 della terza sezione penale.
[95] Introdotto con il d.lgs. 29 dicembre 2017, n. 216, su cui si v. Flor (2018).
[96] Sui reati che potrebbero venire invocati cfr. Bianchi (2016), p. 153; Caletti (2018a), pp. 83 ss.; Schiavon (2017), pp. 185 e 198-199; con riguardo specifico ai reati del *cyberbullo*, Grandi (2017), pp. 46-48 e 52.
[97] Così Verza (2015), p. 17.
[98] Cass. pen. 34357/2017, pt. 3.3 del "considerato in diritto".
[99] Si noti infatti come Cass. pen. 37076/2012 abbia ammesso la configurabilità della fattispecie di violenza sessuale "a distanza".
[100] Legge 19 luglio 2019, n. 69. Si v. a proposito il relativo dossier del Servizio studi del Senato n. 77/2019, "A.S. 1200 e connessi - Disposizioni in materia di tutela delle vittime di violenza domestica e di genere".

La disposizione si propone inoltre di limitare la viralità diffusiva di tali materiali, punendo pure coloro che, avendoli in altro modo ricevuti o acquisiti, mettano in atto le stesse condotte diffusorie (c.d. "secondi distributori"). Si pensi appunto all'ex partner che illegittimamente diffonde gli scatti intimi ricevuti durante la relazione. In tale scenario è tuttavia necessario un dolo specifico, individuato nella volontà di recare nocumento alle persone rappresentate; un requisito, questo, che potrebbe incrinare fortemente l'efficacia della risposta penale[101].

I soggetti passivi non sono soltanto i minori di età bensì, essendo la fattispecie caratterizzata da generale applicazione, qualunque persona. La disposizione fa salvo il caso che il fatto costituisca più grave reato; si noti tuttavia come la sanzione prevista per la pornografia minorile presenti un limite edittale minore (600-ter c.p.: da uno a cinque anni), sicché le condotte di *sexting* secondario aventi ad oggetti immagini di minori finiranno in buona misura nell'ambito applicativo della nuova disposizione. La disposizione non presenta una definizione legale della fattispecie, lasciando così all'esegesi giurisprudenziale la delimitazione della stessa; decisione, questa, che ha trovato il plauso dei primi commentatori[102] alla luce delle difficoltà incontrate in proposito da vari ordinamenti esteri[103]. La fattispecie italiana si limita, come visto, a richiedere che le immagini o i video presentino "contenuto sessualmente esplicito" e siano "destinati a rimanere privati". Il reato è procedibile a querela con un termine di sei mesi e remissione soltanto processuale.

Non irreprensibili sono le circostanze aggravanti previste dalla fattispecie. Le prime due – l'esistenza di un rapporto di coniugio o di relazione affettiva, ovvero l'utilizzo di strumenti informatici o telematici – raffigurano un caso classico di "revenge porn", ove l'ex partner si vendica inoltrando via *smartphone* o mail scatti intimi realizzati durante la relazione. In particolare, con riguardo alla seconda aggravante, pare potersi affermare che essa si presenterà nella maggior parte delle condotte sanzionate, essendo proprio l'utilizzo degli strumenti tecnologici ciò che ha diffuso e al contempo reso tanto pernicioso il fenomeno. Pure la terza aggravante, che ricorre qualora il fatto venga commesso in danno di una persona in condizioni di inferiorità fisica o psichica ovvero di una donna in stato di gravidanza, desta non poche perplessità[104]. Nel complesso, tali circostanze sembrano essere state ampliamente attinte dalla fattispecie di atti persecutori (*stalking*) di cui all'art. 612-bis, probabilmente anche a ragione dell'accelerazione che il procedimento legislativo ha conosciuto a seguito di alcuni casi celebri di "revenge pornography".

Assente è paradossalmente una circostanza aggravante che intervenga qualora la diffusione illecita abbia ad oggetto immagini di un minore. Tale assenza stride fortemente con l'obiettivo della legge, che si propone di tutelare dalla violenza le categorie più deboli della società. Nel caso di vittime minori, la vulnerabilità propria della giovane età incrementa infatti in misura esponenziale le relative conseguenze deleterie sul piano personale e sociale. Tale aspetto risulta particolarmente grave in considerazione del fatto che la nuova disposizione è destinata a trovare applicazione anche in molti casi di diffusione illecita di immagini intime di minori, consensualmente realizzate e poi illecitamente diffuse. L'assenza di una tale aggravante sembra tuttavia conseguire a una scelta (parzialmente) consapevole, in quanto essa è invece presente nella fattispecie di *stalking* da cui sono state altrimenti attinte le circostanze della nuova disposizione. Ipotizzabile è a proposito che il legislatore abbia ritenuto già sufficientemente sanzionate, per il tramite della disciplina di contrasto alla pedopornografia, le condotte che interessino minori, non considerando tuttavia come, a seguito della decisione delle Sezioni Unite del novembre 2018, gli artt. 600-ter e 600-quater non possano più venire in considerazione qualora le immagini siano state originariamente realizzate senza utilizzazione del minore[105].

L'innovazione legislativa si caratterizza anche per l'assenza di strumenti e procedure di facile accesso per un minore di età, al fine di denunciare e reprimere efficacemente i casi che li dovessero coinvolgere. L'Europol ha a tal riguardo rilevato una gravissima carenza di segnalazione di tali situazioni, anche dovuta all'imbarazzo delle giovani vittime e a una possibile

[101] In tal senso Caletti (2018b), che tuttavia ritiene che il ricorso al dolo specifico costituisca un equilibrato punto di approdo.
[102] Caletti (2018b). Dello stesso si v. anche (2018c).
[103] Per alcuni riferimenti alle soluzioni adottate in quegli ordinamenti esteri che già si sono confrontati col fenomeno del *sexting*, cfr. Bianchi (2016), p. 154; in particolare sugli Stati Uniti Salvadori (2017), pp. 802-805; sulla Spagna Villacampa (2017), p. 11, e Caletti (2018a), p. 82; sul Canada Shariff (2015), p. 55.
[104] Per una prima ma approfondita quanto condivisibile analisi delle varie criticità di tale trattamento sanzionatorio, in riferimento al d.d.l. Senato n. 1200 nel frattempo divenuto legge, si rimanda a Caletti (2018b).
[105] In proposito si v. Caletti (2018b).

assenza di consapevolezza che ciò che stanno subendo costituisce un crimine[106]. A riguardo, la legge 71/2017 volta alla prevenzione e al contrasto del cyberbullismo, con cui la nuova disciplina non si coordina espressamente, avrebbe potuto fornire qualche utile esempio[107]. Al contempo, (perlomeno) nel caso di minori sarebbe stato necessario prevedere ulteriori risposte di carattere non penale, volte a prevenire in senso speciale e generale la condotta vietata. Assente nella nuova disciplina è inoltre un'azione preventiva che, per il tramite dei vari ambienti educativi formali e informali, ponga i minori di età in condizione di decidere se, in che termini, con chi e a quali condizioni, (non) scambiarsi immagini sensibili[108].

Da un punto di vista procedurale, infine, la rapidità dell'iter legislativo non ha permesso di considerare adeguatamente né il parere degli esperti, sì da evitare che ad affermarsi fosse una soluzione che poco si attaglia al reale, né la voce dei minori stessi. Come visto, tanto la Convenzione ONU sui diritti del fanciullo, quanto la Carta dei diritti fondamentali dell'UE riconoscono ai minori il diritto di essere sentiti ogniqualvolta siano in preparazione disposizioni legali o nuove politiche che li riguardino.[109] Pur essendo i minori direttamente interessati dalla nuova disposizione, il legislatore non ha tuttavia ritenuto di doverli ascoltare e coinvolgere in maniera sistematica. Al contempo, l'assenza di strumenti di prevenzione e contrasto di carattere non penale male si addice alla tutela dell'interesse superiore del bambino[110]. Un tale affrettato procedimento decisionale pare pertanto, a chi scrive, lesivo sia del diritto partecipativo dei minori a co-determinare la propria esistenza, sia della necessaria tutela dei loro *best interests* – principi, questi, solennemente sanciti a livello tanto internazionale quanto eurounitario. Qualora la nuova fattispecie non sarà in grado di porre effettivo rimedio ai fenomeni di diffusione non consensuale di immagini pornografiche minorili, la situazione italiana continuerà inoltre ad essere caratterizzata da una grave lesione degli obblighi di diritto internazionale ed europeo di protezione dei minori contro l'abuso sessuale.

8. La necessità di una più chiara definizione dei criteri di non punibilità del *sexting*.

In attesa di verificare l'efficacia del nuovo delitto di diffusione illecita di immagini o video sessualmente espliciti, rimane da comprendere in presenza di quali circostanze di fatto le pratiche di *sexting* minorile esulino dall'ambito applicativo della disciplina di contrasto alla pedopornografia. I giudici delle Sezioni Unite hanno a tal proposito indicato alcuni criteri per valutare il carattere non abusivo della condotta e assicurarsi che la realizzazione e lo scambio delle immagini sia frutto di una scelta non caratterizzata da condizionamenti e costrizioni.

Fatto salvo il superamento dell'età del consenso sessuale, ci si chiede *de iure condendo* se la legittimità dello scambio di immagini pornografiche vada verificata caso per caso, oppure se il legislatore dovrebbe prevedere – così com'è il caso per il consenso ad attività sessuali – delle fasce d'età al superamento delle quali il consenso del minore vada considerato scriminante, eventualmente graduando tali soglie in rapporto alla differenza d'età con il partner.[111] Se tale ultima soluzione offrirebbe una maggiore prevedibilità, la valutazione giudiziale permetterebbe un migliore apprezzamento dell'effettiva capacità di discernimento del minore e delle circostanze concrete in cui la condotta si esplica, particolarmente importante in un ambito dove la linea che demarca uno scambio libero da una strumentalizzazione del minore non appare tanto netta. Per evitare tuttavia un'eccessiva discrezionalità della giurisprudenza, e rispondere alle esigenze di prevedibilità, il legislatore dovrebbe perlomeno sancire con maggiore chiarezza gli indici di valutazione dell'"utilizzazione" del minore.

Da verificare sarebbe inoltre l'opportunità di estendere la capacità scriminante anche ai

[106] Europol (2017), p. 21.
[107] Si veda la possibilità, prevista all'art. 2 della legge n. 71/2017, di avanzare al titolare del trattamento dei dati personali, ovvero al gestore di un sito *internet* o di un *social media*, istanza per l'oscuramento, la rimozione o il blocco dei dati personali del minore che abbia subito un atto di *cyberbullismo*.
[108] Sul tema, anche con riferimento ad esperienze estere, si v. i riferimenti *supra* in nota.
[109] Si rinvia nuovamente al parere del Comitato ONU sui diritti dell'infanzia e dell'adolescenza: United Nations Committee on the Rights of the Child (2003), p. 5.
[110] Critica sull'uso di misure repressive penali in casi di *sexting* consensuale tra minori anche l'autorevole voce di Tobin e Parkes (2019), p. 449.
[111] Preferisce tale seconda soluzione Cotelli (2019), p. 14.

partner maggiorenni, qualora la situazione sia priva di comportamenti abusivi, caratterizzata da rispetto reciproco e si inserisca in relazioni perlomeno *in fieri*, presentandosi così – come nel caso di *sexting* tra minorenni – priva di offensività concreta. Diversamente, la limitazione della scriminante nei confronti dei soli minori inciderebbe negativamente in particolare sui c.d. "grandi minori", ovverosia quei giovani prossimi al raggiungimento della maggiore età e che pertanto più facilmente potrebbero presentare partner maggiorenni. Una notevole differenza d'età fra i soggetti richiederà uno scrutinio particolarmente attento a verificare l'eventuale presenza di condizionamenti, pur non potendosi questi risolvere in una presunzione di abusività. Degna di riflessione appare, in conclusione e in termini più generali, la domanda su quali siano le modalità procedurali più efficaci e legittime per maggiormente considerare la voce degli esperti e dei minori stessi al momento della predisposizione di future discipline normative, dando così pieno seguito ai diritti di partecipazione dei minori sanciti a livello internazionale ed eurounitario.

Bibliografia

Agenzia dell'Unione europea per i diritti fondamentali (2017): *Child-friendly justice – checklist for professionals* (Lussemburgo, Ufficio delle pubblicazioni)

Agenzia dell'Unione europea per i diritti fondamentali (2018a): *Mapping minimum age requirements concerning the rights of the child in the EU*

Agenzia dell'Unione europea per i diritti fondamentali (2018b): *Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level - Guidance* (Lussemburgo, Ufficio delle pubblicazioni)

Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa (2015): *Handbook on European law relating to the rights of the child* (Lussemburgo, Ufficio delle pubblicazioni)

Anderson, Monica e Jingjing, Jiang (2018): "Teens' Social Media Habits and Experiences", Pew Research Center

Bertolesi, Riccardo (2018): "Produzione di materiale pornografico: per le Sezioni Unite non è necessario l'accertamento del pericolo di diffusione", *penalecontemporaneo.it*, 30 novembre 2018

Bertolino, Marta (2009): *Il reo e la persona offesa. Il diritto penale minorile*, in Grosso, Carlo Federico, Padovani, Tullio, Pagliaro, Antonio (diretto da), *Trattato di diritto penale*, I (Milano, Giuffrè)

Bertolino, Marta (2010): *Il minore vittima del reato*, 3a ed. (Giappichelli, Torino)

Bianchi, Malaika (2016): "'Il sexting minorile non è più reato?' Riflessioni a margine di Cass. pen., Sez. III, 21.3.2016, n. 11675", *Diritto Penale Contemporaneo – Rivista trimestrale,* 1, pp. 138–154

Bianchi, Malaika (2019): "Produzione di materiale pedo-pornografico: il nuovo principio di diritto delle Sezioni unite", *Archivio penale*, 1, pp. 1-25

Biolcati, Roberta (2010): "Adolescents' online life between experimentation and risk", *Psicologia Clinica dello Sviluppo,* 14, 2, pp. 266–297

Boyd, danah (2008): *Taken Out of Context American Teen Sociality in Networked Publics* (dissertation at the University of Berkeley)

Bulger, Monica, Burton, Patrick, O'Neill, Brian, Staksrud, Elisabeth (2017): "Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online", *New Media & Society,* 19, 5, pp. 750–764

Byrne, Jasmina e Burton, Patrick (2017): "Children as Internet users: how can evidence better inform policy debate?", *Journal of Cyber Policy,* 2, 1, pp. 39–52

Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo, e Papa, Michele (2019): *Trattato di diritto penale – Cybercrime* (Milano, Utet)

Caletti, Gian Marco (2018a): "'Revenge porn' e tutela penale", in *Diritto Penale Contemporaneo – Rivista trimestrale,* 3, pp. 63-100

Caletti, Gian Marco (2018b): "'Revenge porn'. Prime considerazioni in vista dell'introduzione dell'art. 612-ter c.p.: una fattispecie 'esemplare', ma davvero efficace?", *penalecontemporaneo.it*, 29 aprile 2019

Caletti, Gian Marco (2018c): "Al vaglio del Senato il nuovo reato di «diffusione illecita di immagini o video sessualmente espliciti» (c.d. "Revenge porn")", dirittodiinternet.it, 29 aprile 2019

Carr, John (2017): "An open letter to the European Data Protection Supervisor and the Chair of the Article 29 Working Party", eNACSO

Chaudron, Stéphane e Eichinger, Henning (2018): *Eagle-eye on identities in the digital world*, Commissione Europea – Centro comune di ricerca (Lussemburgo, Ufficio delle pubblicazioni)

Commissione Europea (2012): *Impact assessment accompanying the General Data Protection Regulation and the Directive on the protection of individuals*, SEC(2012) 72 final (Bruxelles)

Consiglio d'Europa (2007): *Explanatory Report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)*, Council of Europe Treaty Series, 201

Consiglio d'Europa (2017): *Internet Literacy Handbook* (Strasbourg, Consiglio d'Europa)

Cotelli, Mario (2019): "Pornografia domestica, sexting e revenge porn fra minorenni. Alcune osservazioni dopo la pronuncia delle Sezioni Unite n. 51815/18", *Giurisprudenza Penale Web*, 3

Decker, Scott H. e Marteache, Nerea (eds.) (2017): *International Handbook of Juvenile Justice*, 2a ed. (Cham, Springer)

Delsignore, Stefano (2015): "§ 3 – Pornografia minorile (art. 600-ter c.p.)", in Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo, Papa, Michele (eds.): Trattato di diritto penale, Parte generale e speciale. Riforme 2008-2015 (Milano, UTET), pp. 737–770

Doek, Jaap E. (2019): "The Human Rights of Children: An Introduction", in Kilkelly, Ursula, e Liefaard, Ton (eds.): *International Human Rights of Children* (Singapore, Springer), pp. 3–30

Döring, Nicola (2014): "Consensual sexting among adolescents: risk prevention through abstinence education or safer sexting?", *Cyberpsychology*, 8, 1, article 9

Duru, Boris (2018): *Die Strafbarkeit minderjähriger Personen in den Partikularrechten des Königreichs Italien – mit einem Ausblick auf den Codice Zanardelli von 1889* (Berlin, Lit)

Europol (2017): *Online sexual coercion and extortion as a form of crime affecting children*

Ferla, Lara (2017): "600-ter c.p.", in Forti, Gabrio, Seminara, Sergio, Zuccalà, Giuseppe (eds.): Commentario breve al Codice penale (Milano, Cedam), pp. 1957–1966

Fiandaca, Giovanni e Musco, Enzo (2013): *Diritto penale. Parte speciale. Volume II, tomo primo: I delitti contro la persona* (Torino, Zanichelli)

Flor, Roberto (2018): "La diffusione di riprese e registrazioni di comunicazioni effettuate fraudolentemente: *abusus non tollit usum* (?)", Giurisprudenza italiana, pp. 1733-1744

Grandi, Ciro (2017): "Le conseguenze penalistiche delle condotte di cyberbullismo. Un'analisi de jure condito", Annali online della Didattica e della Formazione Docente, 9, 13, pp. 40–58

Groothuis, Marga M. (2014): "The Right to Privacy for Children on the Internet: New Developments in the Case Law of the European Court of Human Rights", in van der Hof, Simone, van den Berg, Bibi, Schermer, Bart (eds.): Minding Minors Wandering the Web: Regulating Online Child Safety (The Hague, Asser Press and Springer), pp. 143–156

Helfer, Margareth (2007): *Sulla repressione della prostituzione e pornografia minorile* (Padova, Cedam)

Helfer, Margareth (2012): "La pornografia minorile: verso un abbandono dei parametri di un diritto penale del fatto?", Psicoterapia, 32, pp. 283-290

Jasmontaite, Lina e De Hert, Paul (2015): "The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet", *International Data Privacy Law,* 5, 1, 20-33

Kilkelly, Ursula, e Liefaard, Ton (eds.) (2019): *International Human Rights of Children* (Singapore, Springer)

Lamarque, Elisabetta (2016): *"Prima i bambini": Il principio dei best interests of the child nella prospettiva costituzionale* (Milano, FrancoAngeli)

Lansdown, Gerison (2005): *The Evolving Capacities of the Child*, Unicef – Innocenti Research Centre & Save the Children

Lenhart, Amanda (2009): *Teens and Sexting. How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging*, Pew Research Center

Lievens, Eva (2014a): "Bullying and sexting in social networks: Protecting minors from criminal acts or empowering minors to cope with risky behaviour?", *International Journal of Law, Crime and Justice,* 42, 3, pp. 251–270

Lievens, Eva (2014b): "Children and Peer-to-Peer Risks in Social Networks: Regulating, Empowering or a Little Bit of Both?", in van der Hof, Simone, van den Berg, Bibi, Schermer, Bart (eds.): Minding Minors Wandering the Web: Regulating Online Child Safety (The Hague, Asser Press and Springer), pp. 191–210

Lievens, Eva (2017): "Children's rights and media: imperfect but inspirational", in Brems, Eva, Desmet, Ellen, Vandenhole, Wouter (eds.): Children's Rights Law in the Global Human Landscape (New York, Routledge), pp. 231–250

Lievens, Eva, Livingstone, Sonia, McLaughlin, Sharon, O'Neill, Brian, Verdoodt, Valerie (2019): "Children's rights and digital technologies", in Kilkelly, Ursula, e Liefaard, Ton (eds.): *International Human Rights of Children* (Singapore, Springer), pp. 487–513

Livingstone, Sonia e Ólafsson, Kjartan (2011): *Risky communication online*. London School of Economics and Political Science – EU Kids Online

Livingstone, Sonia, Carr, John, Byrne, Jasmina (2016): "One in Three: Internet Governance and Children's Rights", *Discussion Paper of the Unicef Office of Research – Innocenti*, 1/2016

Livingstone, Sonia, Haddon, Leslie, Görzig, Anke, Ólafsson, Kjartan (2011): *EU Kids Online II. Final Report* (London, London School of Economics and Political Science – EU Kids Online)

Livingstone, Sonia, Kirwil, Lucyna, Ponte, Cristina, Staksrud, Elisabeth (2014): "In their own words: What bothers children online?", *European Journal of Communication,* 29, 3, pp. 271–288

Macenaite, Milda (2017): "From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation", in *New Media & Society*, 19, 5, pp. 765–779

Manes, Vittorio (2005): *Il principio di offensività nel diritto penale* (Torino: Giappichelli)

Mantovani, Ferrando (2016): *Diritto penale. Parte speciale*, I, 6a ed. (Milanofiori, Wolters Kluwer)

Mantovani, Ferrando (2016): *Diritto penale. Parte speciale, I, Delitti contro la persona* (Milanofiori: Wolters Kluwer/Cedam)

Mascheroni, Giovanna e Ólafsson, Kjartan (2018): *Accesso, usi, rischi e opportunità di internet per i ragazzi italiani. I primi risultati di EU Kids Online 2017*, EU Kids Online e OssCom

Mazzacuva, Francesco (2017): "I delitti contro lo sviluppo psico-fisico dei minori", in Cadoppi, Alberto, Veneziani, Paolo (eds.): Elementi di diritto penale. Parte speciale, II, I reati contro la persona (Milanofiori: Wolters Kluwer/Cedam), pp. 163-197

Moro, Alfredo Carlo, Dossetti, Maria, Moretti, Carola, Moretti, Mimma, Morozzo della Rocca, Paolo, Vittorini Giuliano, Stefano (2019): *Manuale di diritto minorile*, 6a ed. (Bologna, Zanichelli)

Noto La Diega, Guido (2019): "Grinding Privacy in the Internet of Bodies. An Empirical Qualitative Research on Dating Mobile Applications for Men Who Have Sex with Men", in Leenes, Ronald, van Brakel, Rosamunde, Gutwirth, Serge, De Hert, Paul (eds.): *Data Protection and Privacy: The Internet of Bodies* (Oxford, Hart), pp. 21–69

Palermo Fabris, Elisabetta, Presutti, Adonella, Riondato, Silvio (eds.) (2019): *Diritto penale della famiglia e dei minori*, in Zatti, Paolo (diretto da): *Trattato di diritto di famiglia* (Milano, Giuffrè Francis Lefebvre)

Picotti, Lorenzo (2007): "I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici", in Bertolino, Marta, Forti, Gabrio (eds.): *Scritti per Federico Stella* (Napoli, Jovene), II, pp. 1267-1322

Pistorelli, Luca (2015): "Art. 600-ter", in Dolcini, Emilio, Gatta, Gian Luigi (eds.): *Codice penale commentato, IV edizione* (Milanofiori, Wolters Kluwer), pp. 223–245

Pisu, Alessandra (2019): "Scelte terapeutiche e protezione degli interessi esistenziali del minore nella relazione di cura e nel fine vita", *Giurisprudenza Penale Web*, 1-bis

Reyna, Valerie F. e Farley, Frank (2006): "Risk and Rationality in Adolescent Decision Making", *Psychological Science in the Public Interest,* 7, 1, pp. 1–44

Ringrose, Jessica, Gill, Rosalind, Livingstone, Sonia, Harvey, Laura (2012): *A Qualitative Study of Children, Young People and 'sexting'. A report prepared for the NSPCC*, National Society for the Prevention of Cruelty to Children

Romano, Mario e Grasso, Giovanni (2012): *Commentario sistematico del codice penale*, II, 4a ed. (Milano, Giuffrè)

Rosani, Domenico (2018): "Child's participation online and the General Data Protection Regulation – a dialogue between educational and legal sciences is urgently needed", *merzWissenschaft*, pp. 41–52

Rosani, Domenico (2020): "'We're All in This Together': Actors Cooperating in Enhancing Children's Rights in the Digital Environment after the GDPR", in Leenes, Ronald, Hallinan, Dara, Gutwirth, Serge, De Hert, Paul (eds.): *Data Protection and Privacy: Data protection and Democracy* (Oxford, Hart), pp. 93–126 (in press)

Rosenfeld, Michael J. e Thomas, Reuben J. (2012): "Searching for a Mate", *American Sociological Review,* 77, 4, pp. 523–547

Sacco, Dena T., Argudin, Rebecca, Maguire, James, Tallon, Kelly (2010): *Sexting: Youth Practices and Legal Implications*, Berkman Center for Internet & Society, Harvard University

Salvadori, Ivan (2017): "I minori da vittime ad autori di reati di pedopornografia? Sui controversi profili penali del sexting", *L'indice penale,* pp. 789-837

Salvadori, Ivan (2018): *L'adescamento di minori* (Torino, Giappichelli).

Sassaroli, Giulia (2014): "In tema di detenzione di materiale pornografico realizzato utilizzando minori di anni diciotto: una sentenza assolutoria della Corte d'Appello di Milano", *penalecontemporaneo.it*, 17 giugno 2014

Savirimuthu, Joseph (2016): "Article 8 General Data Protection Regulation: Has Anyone Consulted the Kids?", Blog of the London School of Economics and Political Science

Schiavon, Alessia (2017): "Cat-Fish, Romance Fraud e Sextortion: le nuove frontiere dell'adescamento nei social media", *Informatica e diritto*, 1-2, pp. 177-200

Shariff, Shaheen (2015): *Sexting and Cyberbullying* (New York, Cambridge University Press)

Stanley, Nicky, Barter, Christine, Wood, Marsha, Aghtaie, Nadia, Larkins, Cath, Lanau, Alba, Överlien, Carolina (2018): "Pornography, Sexual Coercion and Abuse and Sexting in Young People's Intimate Relationships: A European Study", *Journal of interpersonal violence,* 33, 19, pp. 2919–2944

Symons, Katrien, Ponnet, Koen, Walrave, Michel, Heirman, Wannes (2018): "Sexting scripts in adolescent relationships: Is sexting becoming the norm?", *New Media & Society,* 20, 10, pp. 3836–3857

Telefono azzurro ed Eurispes (2011): *Indagine conoscitiva sulla condizione dell'infanzia e dell'adolescenza in Italia 2011. Documento di sintesi*

Telefono azzurro ed Eurispes (2012), *Indagine conoscitiva sulla condizione dell'infanzia e dell'adolescenza in Italia 2012. Documento di sintesi*

Tobin, John e Parkes, Aisling (2019): "Art. 13 The Right to Freedom of Expression", in Tobin, John (ed.): *The UN Convention on the Rights of the Child: A Commentary* (Oxford, Oxford University Press)

Unicef (2017): *Children in a digital world* (New York, Unicef)

Unicef Italia (2004): *Convenzione sui diritti dell'infanzia e dell'adolescenza* (Roma, Unicef)

United Nations Committee on the Rights of the Child (2003): *General measures of implementation of the Convention on the Rights of the Child (arts. 4, 42 and 44, para. 6)*, CRC/GC/2003/5 (New York, United Nations)

United Nations Committee on the Rights of the Child (2013): *General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)*, CRC/C/GC/14 (New York, United Nations)

Van der Hof, Simone (2016): "I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World", *Wisconsin International Law Journal,* 34, 2, pp. 409–445

Van der Hof, Simone, van den Berg, Bibi, e Schermer, Bart (2014): *Minding Minors Wandering the Web: Regulating Online Child Safety* (The Hague, Springer)

Verza, Annalisa (2015): "Sulla struttura speculare e opposta di due modelli di abuso pedopornografico", *penalecontemporaneo.it*, 22 aprile 2018, pp. 1-18

Villacampa, Carolina (2017): "Teen sexting: Prevalence, characteristics and legal treatment", *International Journal of Law, Crime and Justice,* 49, pp. 10–21

Zalnieriute, Monika (2019): "Digital rights of LGBTI communities: a roadmap for a dual human rights framework", in Wagner, Ben, Ketteman, Matthias C., Vieth, Kilian (eds.): Research Handbook on Human Rights and Digital Technology. Global Politics, Law and International Relations (Cheltenham: Elgar), pp. 411–433

Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme *online*

Los efectos de la automatización en los modelos de responsabilidad: el caso de las plataformas online

The Effects of Automation on Imputation Models: the Case of Online Platforms

Beatrice Panattoni
Dottoranda di Diritto penale presso l'Università di Verona
beatrice.panattoni@univr.it

Reati informatici | Delitos informáticos | Cybercrimes

Abstracts

Già nella seconda metà del secolo scorso, con lo sviluppo degli agenti informatici e l'apertura al pubblico di Internet, si possono rintracciare le prime applicazioni dell'automazione. La novità tecnologica di questo *medium* ha in questi anni vissuto però importanti e profondi evoluzioni, delineando scenari innovativi e bisognosi di adeguata regolamentazione. Sul fronte dei regimi di responsabilità configurabili in capo ai diversi soggetti, la struttura complessa della rete ha posto numerose problematiche, in particolare per quanto concerne le possibili allocazioni di responsabilità penale in capo agli *Internet service provider*, soggetti privati che gestiscono servizi in rete, il cui ruolo ha visto negli ultimi anni importanti trasformazioni. Partendo dalle novità di rilievo giuridico rinvenibili a livello europeo, si cercherà di evidenziare i più recenti sviluppi in materia. In questa prospettiva, il punto che suscita le maggiori perplessità è quello della configurabilità di una responsabilità penale omissiva a carico degli ISP (*Internet Service Provider*) per contenuti illeciti immessi in rete dagli utenti, ipotesi che rappresenta anche un'occasione, per la dottrina e la giurisprudenza, per interrogarsi su possibili ripensamenti di basilari categorie penalistiche, anch'esse bisognose di adeguarsi alle peculiarità delle componenti tecnico-informatiche.

Ya en la segunda mitad del siglo pasado, con el desarrollo de los agentes informáticos y la apertura de internet al público, se pueden rastrear las primeras aplicaciones de la automatización. La novedad tecnológica de este *médium* ha generado profundas e importantes evoluciones, delineando escenarios innovadores que requieren una adecuada regulación. En relación a los regímenes de responsabilidad personal, la compleja estructura de la red ha planteado numerosos problemas, en particular respecto a los proveedores de servicios de Internet, entidades privadas que gestionan servicios en línea, cuyo papel ha visto importantes transformaciones en los últimos años. A partir de los nuevos problemas legales que se han presentado a nivel europeo, se intentará evidenciar los más recientes desarrollos en esta materia. Desde esta perspectiva, la cuestión que genera el mayor grado de perplejidad es el de la posibilidad de configurar una responsabilidad penal omisiva de los ISP por el contenido ilícito ingresado a la red por los usuarios. La anterior hipótesis representa, además, una oportunidad, tanto para la doctrina como para la jurisprudencia, de cuestionarse sobre un posible replanteamiento de las categorías penales básicas, las cuales debiesen adecuarse a las peculiaridades de los componentes técnico-informáticos.

Since the second half of XX century, thanks to the development of ICT and the opening to the public of the internet, automation has been applied for the first time. The new technologic medium significantly and profoundly evolved over the years, shaping new scenarios that need a proper regulation. With respect to the liability of a

number of subjects, the complexity of the web poses several issues, especially with respect to criminal responsibility (if any) of the Internet service provider, i.e. private entities managing web services, whose role has deeply changed in recent years. Starting from the new legal framework at EU level, this paper aims to highlight the most recent developments on the topic. From the said perspective, a really controversial point refers to a criminal liability for omission of the ISP about the unlawful content uploaded by the users. Such a situation can induce scholars and the case law to rethink basic criminal law concepts, to be reshaped in light of the ICT peculiarities.

Sommario

1. Premessa.

Le componenti tecnologiche, o meglio le nuove tecnologie dell'informazione e della comunicazione (TIC), fondate su algoritmi sempre più complessi, compenetrano ormai in modo incisivo ogni aspetto della vita relazionale: ce ne serviamo per il compimento delle più disparate attività e sono diventate parte integrante di una realtà "collegata"[1]. L'insinuarsi di un elemento "estraneo" ed artificiale, come è appunto quello dell'automazione dei processi di elaborazione dei dati, materializzato nella creazione di strumenti tecnologici sempre più avanzati, ha rivoluzionato la nostra esperienza, suscitando l'interesse di studio delle più diverse branche del sapere.

Uno dei grandi campi di applicazione di queste nuove componenti tecnologiche è costituito dalla costruzione e sviluppo della rete Internet, o meglio del c.d. *Cyberspace*[2]. Diventato oggi luogo sociale, all'interno del quale si svolgono le più disparate attività, il *Cyberspace* ospita un'infinità di relazioni globalizzate, delocalizzate, dilatate e dematerializzate[3].

La rete Internet che conosciamo oggi è considerevolmente cambiata rispetto alle sue prime conformazioni. Grazie all'avvento dei *Big data* e alla *Big data analytics,* il *Web* sta oggi entrando nella sua versione 4.0[4]. Il cambiamento determinante può essere già rintracciato nel massivo passaggio dal dato all'informazione[5], a seguito del quale Internet si presenta come un vero e proprio «villaggio globale»[6], all'interno del quale i singoli utenti possono interagire attivamente, potendo altresì diventare vittime e autori di fatti criminosi[7]. Si tratta oggi di uno «spazio-movimento»[8], uno «spazio mobile in cui tutto cambia rispetto a tutto e in cui la distanza non è niente e la velocità è tutto»[9].

Nel tentativo di analizzare e concettualizzare le diverse novità che caratterizzano l'elemento dell'automazione tecnica operante attraverso agenti informatici, emerge chiaramente come le stesse peculiarità che contraddistinguono la natura e il funzionamento della realtà digitale non possano che avere corrispondenti ricadute sul piano linguistico e concettuale, dal momento che le categorie utilizzate per descrivere, comprendere e regolare tali fenomeni risultano necessariamente permeate dalla loro natura. L'impiego di strumenti informatici e telematici, in quanto portatori di nuove realtà ed esperienze, la cui descrizione e regolamentazione sfugge agli schemi concettuali "tradizionali" (basti pensare alle diverse dimensioni di tempo e spazio del *Cyberspace*), può condurre alla "creazione" di nuovi concetti e categorie;

[1] Definita dal filosofo Luciano Floridi attraverso il neologismo *"onlife"* con il quale si intende definire la realtà che viviamo quale simbiosi tra l'essere *online* e *offline*: la nuova esperienza di una «*hyperconnected reality within which it is no longer sensible to ask whether one may be online or offline*», Floridi (2015); in modo più approfondito Floridi (2017).

[2] Nozione derivante dagli Stati Uniti, la quale non ha preciso contenuto tecnico o giuridico, ma è frequentemente utilizzata per richiamare l'idea del c.d. spazio virtuale quale prodotto dell'integrazione fra sistemi di comunicazione e connessione che utilizzano le nuove tecnologie informatiche, v. Picotti (2011), p. 830. Si tratta di un termine che secondo alcuni è stato utilizzato per la prima volta da William Gibson, nel racconto fantascientifico Burning Chrome (1982) e nel successivo romanzo Nueromancer (1984).

[3] Berlingò (2017), pp. 641-643.

[4] Definito come un *web* "simbiotico". Aghaei (2012), p. 8: «*the dream behind of the symbiotic web is interaction between humans and machines in symbiosis. It will be possible to build more powerful interfaces such as mind controlled interfaces using web 4.0. In simple words, machines would be clever on reading the contents of the web and react in the form of executing and deciding what to execute first to load the websites fast with superior quality and performance and build more commanding interfaces*».

[5] Cassano (2017), p. 1231, con l'espressione "passaggio dal dato all'informazione" si intende che «alla funzione di registrazione e di memorizzazione elettronica dei dati come rappresentazione elementare di un fatto, si affianca l'attività complementare di elaborazione e di organizzazione logica, con formazione di un insieme coordinato di "informazioni"». Nello stesso senso Floridi (2017), p. 96; nonché Berlingò (2017), pp. 641- 675, secondo la quale «il campo d'osservazione è destinato per vero a mutare angolatura appuntandosi più che sul singolo dato, sul processo della c.d. *datafication,* dove tutto è riducibile a informazione e dove la dittatura degli algoritmi rappresenta come scientifiche ed oggettive scelte prodotte da modelli matematico-informatici».

[6] Seminara (1997), p. 72.

[7] Picotti (2012), pp. 2554-2556.

[8] Amato Mangiameli (2017), p. 151.

[9] Ibidem.

oppure, modellando sotto nuove forme esperienze sussumibili entro concetti esistenti (l'investimento di un pedone, accadimento legato alla comune esperienza, ma da parte di un agente autonomo quale una *self-driving car*), può condurre a nuove configurazioni di concetti ancora validi e applicabili.

Il diritto non può dunque rimanere esente da questi mutamenti, evolvendo con il mutare dei mezzi espressivi e delle tecnologie a questi connesse[10]: come la nascita della scrittura ha determinato l'avvento dell'interpretazione, anche la rivoluzione cibernetica non può che coinvolgere la scienza giuridica, in un rapporto di reciproca interazione e condizionamento. Come è stato sostenuto da diverse voci in dottrina[11] infatti, la relazione tra strumento giuridico e tecnologico non deve sfociare in alcuna prevaricazione dell'uno sull'altro, ma il "codice tecnico"[12] deve trovare necessariamente una regolamentazione giuridica che ne plasmi il corso e l'evoluzione entro vie che garantiscano la tutela dei diritti dei soggetti che operano al suo interno o per suo tramite[13].

Tale esigenza è resa ancora più pressante laddove lo strumento di tutela richiesto sia rappresentato dal diritto penale, il cui coinvolgimento nelle dinamiche del *Cyberspace* risulta ormai da numerosi casi giurisprudenziali nonché contributi dottrinali. Essendo infatti il *Cyberspace* caratterizzato da una potenzialità criminale molto elevata[14], data dai suoi caratteri di facile accessibilità, anche in modo anonimo, illimitata diffusione dei contenuti e immediatezza di effetti, la lotta al crimine cibernetico, o meglio ai c.d. «reati cibernetici»[15], è un campo in continuo e necessario aggiornamento.

2. Il *Cyberspace* quale realtà plurisoggettiva.

Nella sua odierna configurazione, il *Cyberspace* si presenta come una realtà in cui operano diversi soggetti, portatori di istanze ed esigenze di tutela diversificate e in un gran numero di casi contrastanti le une con le altre. È possibile individuare tre grandi tipologie di soggetti coinvolti: gli utenti, i *provider* (prestatori di servizi o gestori di piattaforme *online*) e le istituzioni pubbliche.

Occorre precisare che con il termine *provider* si farà qui riferimento alla categoria maggiormente rilevante, ossia ad una particolare tipologia di *Internet service provider* (prestatori di servizi in rete): gli *hosting provider,* intermediari che gestiscono servizi di memorizzazione di dati altrui[16] attraverso piattaforme di *social network, blog* o altre tipologie di siti internet.

Il ruolo degli utenti e dei *provider* è considerevolmente cambiato nel tempo, le capacità e le potenzialità di queste due categorie si sono ampliate e articolate attraverso modalità nuove e disparate.

Per quanto riguarda gli utenti, vi è stato un cambiamento sia sul piano qualitativo sia su quello quantitativo. Sotto il primo profilo, nell'era del web 4.0, essi sono divenuti parte interattiva nel *Cyberspace,* vengono spesso definiti quali *prosumer*[17], produttori e non solo fruitori di contenuti e servizi *online*. Sotto il secondo profilo, il numero di utenti che interagiscono in rete è esponenzialmente aumentato[18], grazie alle capacità di accesso continuo, rese possibili dai

[10] Pascuzzi (2016), p. 12.
[11] Picotti (2019), pp. 33-96; nello stesso senso Fiandaca (2005), p. 7-23; nonché Luberto e Zanetti (2008), p. 497 ss., secondo il quale il diritto può «incidere sull'architettura – intesa come insieme delle caratteristiche tecniche, comprensive del *software* e dell'*hardware*, che rendono la rete così com'è – e regolare i comportamenti degli utenti».
[12] Lessing (2006).
[13] Applicazione di questo approccio è la c.d. *privacy by default* e *by design* regolata dal GDPR. Sul punto Finocchiaro e Avitabile (2017).
[14] Gli atti delittuosi all'interno del *Cyberspace* coinvolgono ormai un gran numero di settori e fattispecie criminose. Essi possono essere suddivisi, come riportato in Sabella (2017), pp. 149-151, in: *Cybercrime* comune; *Cyber hactivism; Cyber espionage; Cyber war; Cyber terrorism.*
[15] Definiti quali reati che «si commettono o si possono commettere in rete o nel *web* o, meglio "nel" *Cyberspace,* in quanto la formulazione legale delle relative fattispecie incriminatrici contiene un elemento essenziale o circostanziale che *espressamente* richiama la rete ("reati cibernetici in senso stretto"), ovvero prevede elementi di tipizzazione del "fatto" di reato che solo *implicitamente* od in via ermeneutica sono *compatibili* con la concreta realizzazione nel *Cyberspace* ("reati cibernetici in senso ampio")»; così Picotti (2019), pp. 77-78.
[16] Così come definiti dall'art. 14 della direttiva 31/2000/UE (c.d. direttiva sul commercio elettronico, o direttiva *e-commerce*), relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno: prestatori di un «*servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio*».
[17] Gli utenti che producono in modo amatoriale contenuti a cui hanno accesso anche gli altri utenti vengono chiamati *prosumer*, crasi dei termini *producer* e *consumer*; si tratta di un termine introdotto da Alin Toffler nel 1980 (A. Toffler, *The third wave*, New York, 1980), così come viene riportato in Montanari (2017), p. 260; nello stesso senso Scialdone (2013), p. 8.
[18] Nel marzo 2018 il fondatore di Facebook annunciava che gli utenti iscritti al suo *social network* avevano raggiunto i 2,2 miliardi (https://www.facebook.com/zuck/posts/10104878807622211).

numerosi dispositivi elettronici, i quali sono ormai parte integrante della quotidianità.

Anche gli *Internet Service Provider* (ISP) hanno conosciuto importanti cambiamenti sul fronte degli strumenti tecnici a loro disposizione, i quali hanno contribuito ad accrescere le loro potenzialità e il loro ruolo nella Rete. Andando ben oltre il mero servizio di memorizzazione di informazioni, questi soggetti si sono ormai allontanati dalla definizione contenuta nella direttiva europea sull'*e-commerce*, la cui disciplina risulta – come si vedrà meglio *infra* – non più adeguata ai tempi[19]. L'evoluzione più importante risiede nel cambiamento della loro posizione rispetto ai contenuti presenti sulle piattaforme da essi gestite, non più fondata su mere operazioni automatizzate, tecniche e passive, essendo piuttosto divenute "attive", come rilevato dalla stessa giurisprudenza europea e nazionale[20].

La continua ed inarrestabile crescita del web e della mole di contenuti che in esso vengono quotidianamente immessi, trasportati e memorizzati, è stata in gran parte resa possibile dalle nuove attività svolte dai *provider*. Quelle che assumono maggiore rilevanza sono, per l'appunto, quelle che si basano sull'automazione tecnologica di analisi, organizzazione e relazione dei contenuti memorizzati, che rendono possibile agli ISP il trattamento delle informazioni desiderate[21], reperendole sempre più facilmente all'interno dell'«oceano informativo»[22]. Si tratta di attività che vengono utilizzate dagli intermediari per lo svolgimento del proprio esercizio economico (si pensi alla "profilazione" dell'utente a scopi pubblicitari). Lo sviluppo tecnologico ha reso dunque possibile l'acquisizione di maggiori capacità di controllo ed intervento da parte dei prestatori di servizi *online,* seppur ogni situazione vada considerata nella sua singolarità, dal momento che il grado di incidenza e di operatività nella rilevazione e controllo dei contenuti mutano in base alle tipologie di *softwares* utilizzati, ai servizi e alle *policies* di gestione scelte dall'ISP[23].

L'interazione tra il ruolo maggiormente partecipativo degli utenti e le capacità di gestione ed elaborazione dei dati dei *provider* ha determinato la creazione di nuove tipologie di piattaforme *online*, come i motori di ricerca ed i siti ospitanti i c.d. *user generated content*[24], contenuti che vengono direttamente creati dagli utenti (come accade nei *social network*). Queste ultime sono le realtà che pongono le maggiori problematiche dal punto di vista giuridico: ci si interroga infatti se gli ISP possano essere ritenuti responsabili per i contenuti illeciti caricati, o anche condivisi dai propri utenti, dovendo altresì distinguere tra *user generated content* e *user uploaded content,* contenuti altrui solamente riprodotti *online* senza alterazioni o rielaborazioni[25].

Vi è infine la terza categoria di soggetti coinvolti nelle dinamiche del *Cyberspace,* quella delle istituzioni ed autorità pubbliche, le quali cercano di regolare l'utilizzo ed il funzionamento della rete, sorvegliare le attività che vi si svolgono ed in specie contrastare la criminalità cibernetica attraverso misure preventive od attività investigative.

Per incentivare e strutturare il coinvolgimento del soggetto pubblico, è particolarmente rilevante la scelta di istituire autorità amministrative competenti nei specifici settori d'interesse, così che prestatori di servizi in rete ed utenti possano avere un ente pubblico quale punto di

[19] Secondo diverse voci della dottrina la direttiva 31/2000/CE necessita di un ripensamento o quantomeno aggiornamento; si tratta infatti di una normativa che si trova oggi a disciplinare una realtà diversa – portatrice quindi di differenti esigenze di tutela – rispetto a quella risalente al periodo storico in cui è entrata in vigore. Sul punto: Picotti (2019), pp. 81-89; Petruso (2018), pp. 511-558; Bocchini (2017), pp. 632-643; Pollicino (2014), pp. 1-27.

[20] Corte di giustizia dell'Unione Europea, sentenza del 23 marzo 2010, cause riunite da C-236/08 a C-238/08, *Google France e Google*, EU:C:2010:159; sentenza del 12 luglio 2011, C-324/09, *L'Oréal e a.,* EU:C:2011:474. Secondo questa giurisprudenza occorre distinguere tra *provider* c.d. "attivi" e passivi, dal momento che gli intermediari possono andare esenti da responsabilità – secondo il regime delineato dalla direttiva *e-commerce* – solo se mantengano un comportamento di rigorosa passività nei confronti dei contenuti da essi conservati od ospitati.

[21] Si pensi ai c.d. programmi filtro, *software* «in grado di controllare i contenuti dei materiali che gli utenti immettono in rete tramite il servizio reso dal *provider*», Di Ciommo (2010), p. 831.Oltre a questi sono attualmente utilizzati dagli ISP numerosi algoritmi e *software* di riconoscimento e monitoraggio dei dati, cfr. nota 39.

[22] Bugiolacchi (2013), p. 205.

[23] Di Ciommo (2010), pp. 830-833. La capacità di controllo dipende inoltre dal tipo di *provider*. Per i soggetti che forniscono l'accesso alla rete vi sono possibilità di controllo sia attraverso un esame delle informazioni prima del loro trasferimento che in tempo reale; mentre alcuni *service provider* possono anche non operare un controllo delle informazioni fornite.

[24] Termine che si è iniziato a utilizzare intorno al 2005, con la diffusione delle piattaforme sociali. Secondo l'OCSE, per essere qualificato come *user generated content* un contenuto deve essere: (i) pubblicamente accessibile su un sito Internet o un *social network;* (ii) il risultato di un certo apporto creativo; (iii) creato al di fuori di attività professionali o imprenditoriali. Organization for Economic Co-operation and Development, *Participative web: user-created content,* DSTI/ICCP/IE(2006)7/FINAL, 12.04.2007, disponibile al sito https://www.oecd.org/sti/38393115.pdf. Secondo invece l'Ofcom (Office of Communications, l'autorità competente e regolatrice indipendente per le società di comunicazione nel Regno Unito) si tratta di contenuti multimediali resi disponibili *online*, derivanti da un'attività creativa che non è la principale e diretta fonte di guadagno dell'autore. Ofcom, *The Value of User Generated Content,* 21 June 2013, p. 5, disponibile al sito https://www.ofcom.org.uk/__data/assets/pdf_file/0016/32146/content.pdf. Sul punto cfr. D'Ippolito (2017), pp. 524-529.

[25] Ibidem.

riferimento a cui ricorrere in caso di necessità. Autorità di questo tipo sono già oggi esistenti, un esempio si può rintracciare in tema di lotta alla pedopornogragia *online*: in questo ambito l'art. 14 *bis* della legge n. 269 del 3 agosto 1998, introdotto dalla L. n. 38/2006, ha previsto l'istituzione del Centro nazionale per il contrasto della pedopornografia sulla rete Internet[26]. Ulteriori interventi in questo senso sono stati fatti anche in materia di lotta al terrorismo, campo nel quale la collaborazione tra istituzioni pubbliche e soggetti privati si è fatta sempre più stringente[27].

In quanto realtà plurisoggettiva il *Cyberspace* costituisce un contesto nel quale si scontrano diverse esigenze, portartici di diversi diritti ed interessi di difficoltoso contemperamento, e nel quale è quindi complesso attribuire in modo generalizzato forme di responsabilità ai singoli soggetti. Uno degli aspetti più controversi si sostanzia nel complesso bilanciamento tra i diritti facenti capo agli utenti, vittime di crimini cibernetici – i cui diritti dovrebbero essere garantiti e protetti attraverso l'intervento di autorità pubbliche e non (soltanto) enti privati – e gli interessi degli ISP esercenti attività di libera impresa nel *Cyberspace.* La complessità nasce soprattutto dal tradizionale approccio dicotomico che contrappone due istanze in termini contrastanti, come nel caso più frequente di conflitto tra diritto alla libertà d'espressione e tutela dei diritti della personalità, quando (anche in rete) gli uni sono strumentali all'esercizio degli altri ed è, dunque, ancor più delicata l'attribuzione di prevalenza ad uno di essi[28].

Le tre categorie di soggettività sopra richiamate, in considerazione delle modalità di realizzazione delle proprie attività in rete o per la loro natura pubblicistica, sono parti imprescindibili per la costruzione di una equilibrata regolamentazione delle responsabilità nel *Cyberspace*. In questo ambiente, per la stessa evoluzione che lo sta segnando, sembra infatti difficile allocare una generale responsabilità per violazioni e contenuti illeciti in capo ad un singolo attore o categoria di attori, emergendo molto spesso l'utilità delle teorie del *"risk sharing"* e del *"problem of many hands"*[29].

Non considerare questa interazione tra le diverse soggettività nel delineare una forma di regolamentazione fondata su un sistema normativo "integrato" e multilivello[30] può, da una parte, creare incertezze applicative, dall'altra, lasciare troppa discrezionalità in capo a soggetti privati, quali appunto gli ISP, che agiranno in ogni caso seguendo logiche economico-imprenditoriali. Il paradigma economico su cui si fondano le scelte operative dei prestatori di servizi *online* guarda infatti all'*audience* come a una «vera e propria merce di scambio, dal momento che il potere della stessa è prodotto, venduto, acquistato e consumato»[31]. Considerando che le nuove tecnologie di *user data profiling* rendono possibile la predisposizione di pubblicità mirate e calibrate in base alle preferenze degli utenti[32], i cui dati diventano sempre più preziosi nel mercato digitale, le scelte degli ISP saranno sempre più dirette all'incremento del numero di utenti che usufruiscano dei servizi e delle piattaforme da essi gestiti. E una tale logica non può che condurre a dei rischi per i diritti della persona e a dei vuoti di tutela, dal momento che elevati numeri di utenti possono essere attirati dall'alto grado di libertà e autonomia che il gestore della piattaforma concede loro nel caricamento di contenuti o, nei casi più gravi,

[26] Centro istituito presso il servizio di Polizia postale e delle comunicazioni del dipartimento della Pubblica Sicurezza a Roma, che ha il compito di raccogliere tutte le segnalazioni, provenienti da organi di polizia stranieri, da soggetti pubblici, da associazioni di volontariato, da *provider* e da privati cittadini, riguardanti siti che diffondono materiale pedopornografico, ma anche gestori o eventuali beneficiari che, in caso di riscontro positivo, vengono inseriti dalla Polizia in un elenco tenuto costantemente aggiornato, la cosiddetta *"black list"*. Tale elenco viene poi fornito agli ISP, che provvedono ad inibire la navigazione attraverso sistemi tecnici di filtraggio. Sul punto cfr. Picotti (2007), pp. 1196-1211.

[27] Si pensi al d.l. n. 7 del 18 febbraio 2015, con il quale è stata prevista la redazione di un elenco di siti web utilizzati per attività e condotte di associazione terroristica da parte dell'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, nonché l'obbligo per i fornitori di connettività di inibire l'accesso ai siti inseriti nella lista quando ne faccia richiesta la magistratura, (sul punto Scardino (2015), pp. 215-239). Per esperienze in altri ordinamenti, si pensi alla legge francese che ha introdotto un obbligo per gli intermediari (ma non per i *social network*) di rimozione o blocco di tutti i siti che inneggiano all'apologia al terrorismo sulla base di una *black list* predisposta da un organo *ad hoc* del Ministro degli Interni (*Decret* n. 2015-125 *du fevrie* 2015, http://www.legifrance.gouv.fr, (sul punto Abbondante (2017), p. 64).

[28] Di Tano (2017), p. 126. Sul tema del bilanciamento dei diritti fondamentali in rete si è espressa più volte la Corte europea dei diritti dell'uomo, si ricordano le seguenti pronunce: *Neij e Sunde Kolmisoppi v. Sweden (The Pirate Bay),* ricorso n. 40397/12, sentenza del 19/02/2013; *Delfi AS v. Estonia,* ricorso n. 64569/09, sentenza del 16/06/2015; *Pihl v. Sweden,* ricorso n. 74742/14, sentenza del 9/03/2017.

[29] Helberger *et al.* (2018), pp. 1-14.

[30] Sabella (2017), pp. 140-142.; Militello (2014), pp. 106-132

[31] Smythe (2009), pp. 238-240; così come riportato in Montanari (2017), p. 261.

[32] Molti intermediari traggono profitto dalla raccolta dei dati personali e sensibili degli utenti, di cui gli inserzionisti pubblicitari si servono per individuare i profili a cui destinare pubblicità mirate in base a gusti, preferenze e attitudini. Inoltre, gli intermediari possono evidenziare contenuti popolari (i quali registrano grandi numeri di interazioni), concentrando intorno a questi ultimi pubblicità mirate. Cfr. Allegri (2017), pp. 70-72.

potrebbero essere attirati dagli stessi contenuti illeciti ospitati dalla piattaforma.

La giurisprudenza, europea e nazionale, nonché i contributi dottrinali che hanno affrontato il tema delle responsabilità nel *Cyberspace,* si sono concentrate nel tempo proprio sulla complessa tematica della responsabilità dei prestatori di servizi[33]. È infatti su questi ultimi, in virtù del ruolo di primaria importanza che rivestono nella gestione della realtà digitale, che si concentrano i dubbi relativi ad attribuzioni di forme di responsabilità per gli illeciti commessi tramite le piattaforme ed i servizi da loro offerti.

L'esigenza di una maggior responsabilizzazione di questi soggetti[34] – i cui termini e condizioni saranno analizzati in seguito – si fonda quindi non solo sulla loro posizione di «custodi materiali»[35] dei contenuti della rete, ma soprattutto sulle capacità di intervento di cui dispongono e che attualmente già utilizzano, senza che queste possano dunque considerarsi fonte di costi eccessivi da sostenere. L'attività di rilevazione ed analisi dei contenuti illeciti *online* all'interno delle piattaforme può essere infatti effettuata grazie a *softwares*, i quali, «basati sull'utilizzo di 'impronte digitali' abbinate univocamente al contenuto digitale tutelato, non richiedono irragionevole impiego di risorse preposte allo scopo»[36]. Inoltre, gli ISP di grandi dimensioni dispongono già di *staff* di persone dedicate alla gestione delle segnalazioni concernenti contenuti illeciti presenti sulle proprie piattaforme[37]. Naturalmente regimi di responsabilità fondati su tali capacità devono partire necessariamente da una distinzione fra le diverse tipologie di intermediari, differenziando quelli più solidi da un punto di vista imprenditoriale ed economico da quelli di più modeste dimensioni e strutture tecniche, in modo da evitare che un regime troppo severo di responsabilità espella dal mercato i *provider* «non in grado di sopportare i costi di un sistema capillare di prevenzione degli illeciti oppure di un allargamento del fronte dei risarcimenti dovuti»[38].

3. La responsabilità penale degli ISP in caso di caricamento e/o diffusione di contenuti illeciti in rete.

Gli *hosting provider* assumono un ruolo di particolare rilevanza nei casi in cui vengano caricati e diffusi per il tramite delle piattaforme da questi gestite contenuti aventi carattere lesivo di diritti altrui. Si tratta, in particolare, di quei reati cibernetici commessi attraverso la comunicazione di informazioni in rete, o, meglio, attraverso la «messa a disposizione» di dati in rete[39]. Tra le fattispecie maggiormente rilevanti basti qui richiamare il reato di diffamazione

[33] Anche se recentemente l'attenzione si è spostata anche sugli utenti, in quanto autori materiali degli illeciti commessi nel *Cyberspace.* Sul punto giova richiamare la proposta di legge a firma del senatore Nazario Pagano (atto n. 895 Senato) la quale propone di introdurre un obbligo di identificazione degli utenti, aggiungendo all'interno del D.lgs. n. 70/2003 (attuativo della direttiva sull'*e-commerce* 31/2000) l'art. 16 *bis,* ai sensi del quale «*1. I fornitori di servizi di memorizzazione permanente hanno l'obbligo di richiedere, all'atto di iscrizione del destinatario del servizio, un documento d'identità in corso di validità. 2. L'inosservanza dell'obbligo di cui al comma 1 comporta l'irrogazione di una sanzione amministrativa pecuniaria da 500 a 10.000 euro. 3. Le sanzioni amministrative pecuniarie di cui al comma 2 sono applicate dall'Autorità per le garanzie nelle comunicazioni con provvedimento motivato, previa contestazione degli addebiti agli interessati, da effettuare entro un mese dall'accertamento. 4. Le disposizioni del presente articolo si applicano a decorrere dal 1° gennaio 2020*».

[34] In questo senso, nella giurisprudenza europea: Corte di giustizia europea, sentenza del 23 marzo 2010, cause riunite da C-236/08 a C-238/08, *Google France e Google*, EU:C:2010:159; sentenza del 12 luglio 2011, C-324/09, *L'Oréal e a.,* EU:C:2011:474; sentenza del 27 marzo 2014, C-314/12, *UPC Telekabel Wien,* EU:C:2014:192. Nella giurisprudenza italiana: Corte d'Appello di Roma, 19 febbraio 2018, n. 1065, inedita; Corte d'Appello di Roma, 28 aprile 2017, n. 2833, in *Quotidiano giuridico,* 10 maggio 2017; Tribunale di Torino, 7 aprile 2017, n. 1928, in *Danno resp.*, 2018, 1, p. 87 ss.; Tribunale di Napoli Nord, 3 novembre 2016, in *Giur. it.*, 2017, 3, p. 629 ss.; Tribunale di Milano, 7 giugno 2011, n. 7680, inedita.

[35] Di Tano (2017), p. 114.

[36] Tosi (2017), pp. 75-122. Altri esempi possono essere il blocco dei numeri IP e la manomissione o blocco del DNS (*Domain Name Server*), con il limite tuttavia di impedire l'accesso a qualsiasi contenuto, anche se innocuo, ospitato su un sito oscurato. Inoltre, si ricordano alcuni strumenti già utilizzati da alcuni *provider:* l'algoritmo di *scaling* multimediale (MDS) per rappresentare e individuare la somiglianza tra siti contenenti espressioni d'odio; il *software* Perspective, che utilizza modelli di apprendimento automatico per rilevare automaticamente insulti, molestie e parole ingiuriose, valutandone il grado di nocività in modo più accurato e veloce; l'algoritmo Edgerank, che valorizza taluni contenuti in base al numero e alla frequenza delle interazioni fra gli utenti; gli algoritmi di Instagram e Twitter che organizzano i contenuti in base alle preferenze degli utenti e non alla cronologia del caricamento; il *software* Content ID con cui YouTube esamina ogni video caricato e lo confronta con un database di file realizzato in accordo con i titolari dei diritti d'autore.

[37] Di Tano (2017), p. 121.

[38] Piraino (2017), p. 155.

[39] Il principio che fa coincidere, nei casi di comunicazioni illecite in rete, il momento in cui il comportamento commesso *online* assume rilevanza giuridica con il momento della "messa a disposizione" dei dati è ricavabile dalla legge tedesca del 22 luglio 1997 sui servizi di informazione e telecomunicazione, così come analizzata da Picotti (1999) pp. 379-380.

online ex art. 595 c. 3 c.p[40].; il reato di diffusione di materiale pedopornografico ex art. 600 *ter* c. 3 c.p.[41]; il reato di istigazione o apologia a commettere reati ex art. 414 c.p., il quale ha assunto particolare rilevanza in materia di lotta contro il terrorismo[42]; nonché, da ultimo, anche il reato di diffusione illecita di immagini o video sessualmente espliciti ex art. 612 *ter* c. 3 c.p.[43].

Occorre precisare che tra gli *hosting provider* qui presi in considerazione si escluderanno le c.d. testate telematiche, le quali si differenziano in virtù del particolare servizio che offrono. Non verrà dunque presa in considerazione la problematica legata all'eventuale applicabilità del regime delineato dall'art. 57 c.p.[44], che non può che escludersi nei casi esaminati, rilevando per i soli servizi *online* di informazione professionale, in virtù dell'equiparabilità funzionale e ontologica degli stessi con la stampa tradizionale[45].

Il regime di responsabilità penale del *provider* in questi casi può distinguersi sulla base della condotta posta in essere dallo stesso. Non costituiscono casi di dubbia ricostruzione dogmatica le ipotesi di condotte commissive – quali quelle di caricamento, condivisione o modifica di dati – integranti reato, poste in essere dallo stesso ISP. Il prestatore di servizi risponderà infatti in quanto autore o co-autore della «messa a disposizione» o della diffusione di contenuti illeciti[46].

La condotta commissiva penalmente rilevante dell'ISP in questi ultimi casi dovrà però consistere nell'immissione (o diffusione) dolosa di dati, a seguito di un vaglio contenutistico degli stessi, non potendo essere ritenuta sufficiente la mera predisposizione dei supporti tecnici di funzionamento della rete, la fornitura degli accessi o la gestione delle piattaforme *online*. Le attività normalmente poste in essere dagli ISP vengono infatti considerate quali giuridicamente legittime e socialmente adeguate, non determinando di per sé il pericolo di verificazione dell'evento offensivo tipico[47].

Di maggiore interesse sono i casi in cui la condotta attribuibile all'intermediario sia di natura omissiva, per la quale egli potrà rispondere o a titolo autonomo secondo il paradigma dell'art. 40 cpv. c.p. o, per combinato disposto con l'art. 110 c.p., a titolo di concorso omissivo nel reato realizzato dall'utente, ipotesi resa particolarmente rilevante dalle nuove tipologie di piattaforme e servizi *online* descritte in precedenza, in cui il ruolo dell'utente è evoluto da passivo ad attivo.

Prima di procedere occorre tuttavia distinguere due differenti ipotesi: la condotta omissiva del prestatore di servizi può infatti consistere, da una parte, nel mancato controllo e censura preventiva del contenuto illecito caricato o diffuso da un proprio utente sulla piattaforma; o, dall'altra parte, nella mancata rimozione dello stesso contenuto, pubblicamente accessibile sul proprio sito *web*. Si profilano dunque due diverse ipotesi di responsabilità: una *ex ante,* operante prima che i dati vengano resi disponibili in rete; una *ex post*, legata alla fase di perdurante disponibilità che caratterizza le informazioni caricate nel *web*.

La prima ipotesi di responsabilità è esclusa dalla maggioranza della giurisprudenza[48] e della dottrina. In particolare, è stato evidenziato come non sarebbe riscontrabile *de jure condito*

[40] La giurisprudenza è conforme nel ritenere Internet, in virtù della sua potente diffusività e pubblicità, elemento compreso nella definizione «*qualsiasi altro mezzo di pubblicità*», legittimando l'applicazione della fattispecie aggravata del reato di diffamazione ex art. 595 c. 3 c.p.. In questo senso: Cass. Pen., sez. V., 27 dicembre 2000, n. 4741, in *Crit. dir.*, 2000, p. 504 ss.; Cass. Pen., sez. I, 15 marzo 2011, n. 16307, in *Guida al diritto,* 2011, 24, p. 71 ss.; Cass. Pen., sez. I, 21 dicembre 2010, in *Cass. pen.,* 2011, p. 4315 ss.; Cass. Pen., sez. V, primo febbraio 2017, n. 4873, in *Foro it.,* 2017, p. 251 ss.. In dottrina: Tabarelli de Fatis (2013), p. 221; Curreli (2017), p. 189-191.

[41] In materia cfr. Picotti (2006), p. 175; Delsignore (2019), p. 446.

[42] Flor (2017), p. 325.

[43] Fattispecie di reato che è stata introdotta nel codice penale dalla L. del 19 luglio 2019, n. 69 (c.d. Codice rosso), approvato definitivamente dal Senato il 17 luglio 2019. Per un'analisi più ampia: Caletti (2018), pp. 63-100.

[44] La giurisprudenza di legittimità ha evidenziato più volte la profonda differenza che sussiste tra testate telematiche *online* e altri siti *web* veicolanti informazioni, come *blog*, *forum* o *social network*. Da ultimo: Cass. pen., 1° febbraio 2017, n. 4873 in *Foro it.,* 2017, n. 4, p. 258 ss.; Cass. pen., 23 gennaio 2019, n. 3148, in *Dir. inf.*, 2018, n. 6, p. 901 ss.

[45] L'evoluzione giurisprudenziale in materia è stata altalenante: (i) in una prima stagione la giurisprudenza di legittimità aveva escluso l'applicabilità dell'art. 57 c.p. ai direttori delle testate telematiche (Cassazione n. 35511 del 1° ottobre 2010 e n. 44126 del 29 novembre); (ii) la pronuncia a Sezioni Unite del 20 luglio 2015, n. 31022, ha optato per la riconducibilità delle testate giornalistiche *online* nella definizione di stampa, estendendo a queste ultime le garanzie costituzionali previste per la carta stampata; (iii) recentemente, con la pronuncia dell'11 gennaio 2019, n. 1275, la Corte ha ritenuto applicabile alle testate telematiche anche il regime delineato dall'art. 57 c.p. (commento a questa ultima pronuncia: Mauri (2019), disponibile al sito: www.penalecontemporaneo.it). Criticamente sull'analogia *in malam partem*: Catullo (2019); Petrini (2017).

[46] Seminara (1997), pp. 96 ss.; Ruggiero (2001), pp. 586-602; Petrini (2004) p. 151; Bartoli (2013), p. 604.

[47] Sieber (1997), pp. 1206-1212; Ruggiero (2001), p. 591.

[48] Corte di giustizia europea, sentenza del 24 novembre 2011, C-70/10, *Scarlet Extended*, EU:C:2011:771; sentenza del 16 febbraio 2012, C-360/10, *SABAM*, EU:C:2012:85; Corte europea dei diritti dell'uomo, 9 marzo 2017, *Pihl c. Svezia*. Nella giurisprudenza nazionale basti richiamare il noto caso Google c. ViviDown, Cass. Pen., Sez. III, 17 dicembre 2013, n. 5107, in *Dir. fam.*, 2014, 2, p. 675 ss.

alcuna fonte giuridica che preveda a carico degli intermediari un obbligo di impedire il reato. Riassumendo brevemente le argomentazioni di questo orientamento[49], ad ostacolare l'attribuzione di una posizione di garanzia in capo a tali soggetti vi sarebbe, in primo luogo, il divieto di imporre un obbligo generale di controllo preventivo stabilito dalla direttiva *e-commerce* e attuato dall'art. 17 D.lgs. n. 70/2003, il quale prevede espressamente che i prestatori di servizi in rete non possano essere assoggettati ad un obbligo generale di sorveglianza sulle informazioni trasmesse o memorizzate, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite[50]. Un simile obbligo richiederebbe ai *provider* di porre in essere un'attività eccessivamente onerosa, inesigibile e tecnicamente irrealizzabile (un controllo e filtraggio di tutte le informazioni che passano attraverso un *server* sarebbe infatti impraticabile).

In secondo luogo, oltre a non ritenersi configurabile in capo a tali soggetti una posizione di protezione o di controllo[51], essi non disporrebbero nemmeno di specifici poteri impeditivi che consentirebbero loro di impedire o interferire con il realizzarsi della condotta dell'autore del reato.

Seppure quest'ultimo punto susciti qualche perplessità – sulle quali ci si soffermerà in seguito –, in effetti, se si guarda alla responsabilità *ex ante* degli intermediari, gli orientamenti giurisprudenziali, nonché le recenti evoluzioni europee in materia[52], conducono all'esclusione di una sua configurabilità, in particolare per le criticità a cui condurrebbe un filtraggio in entrata dei colossali quantitativi di dati che transitano sui *server* dei diversi prestatori di servizi in rete. L'onerosità che caratterizzerebbe un tale obbligo minerebbe gravemente il diritto alla libertà d'impresa, tutelato dall'art. 16 della Carta di Nizza, facente capo agli ISP[53]. Inoltre, il sistema potrebbe non distinguere sempre le comunicazioni lecite da quelle illecite, rischiando così di compromettere il diritto fondamentale degli utenti alla libertà di ricevere o di comunicare informazioni, tutelato dall'art. 11 della Carta di Nizza[54].

Rimane dunque da verificare la configurabilità della seconda ipotesi sopra individuata, integrante una responsabilità dell'intermediario *ex post*. Ed è proprio questa che suscita il maggior interesse, nonché numerosi dubbi.

Sospendendo per un momento l'analisi della configurazione che questa seconda ipotesi di responsabilità possa assumere secondo i dettami dell'ordinamento penalistico interno, è necessario proseguire tenendo conto del quadro europeo normativo di riferimento che si sta delineando negli ultimi tempi. Dai recenti interventi che coinvolgono la figura degli intermediari a livello europeo emerge infatti come la valorizzazione del ruolo degli ISP nella regolamentazione delle attività nel *Cyberspace* sia sempre più connessa al periodo di perdurante disponibilità di contenuti illeciti in rete.

L'importanza del tema della responsabilità degli intermediari è stata infatti colta dalle istituzioni europee, le quali si sono fatte promotrici di diversi interventi mirati ad un aggiornamento della disciplina (ferma alla direttiva *e-commerce* del 2000) che li riguarda. Anche la figura dell'ISP si inserisce, infatti, all'interno della Strategia per il Mercato Unico Digitale dell'Unione Europea[55], e tale consapevolezza ha condotto a diverse Comunicazioni e Raccomandazioni della Commissione, il cui contenuto tende ad integrare e attualizzare i vari punti irrisolti in tema di responsabilità degli operatori nel *Cyberspace*.

[49] Seminara (1998), pp. 745-774; Seminara (2014), pp.594-605; Manna (2001), pp. 145-151; Ruggiero (2001), pp. 586-602; Petrini (2004); Spagnoletti (2004), pp. 1922-1937; Ingrassia (2012), pp. 47-67.
[50] È da evidenziarsi tuttavia che la tenuta di questo divieto è stata di recente messa in discussione nella domanda di pronuncia pregiudiziale proposta alla Corte di Giustizia europea dall'*Oberster Gerichtshof* il 10 gennaio 2018, nella causa Eva Glawischnig-Piesczek/Facebook Ireland Limited (Causa C-18/18).
[51] Petrini (2004), p. 169; Bartoli (2013), p. 603.
[52] Cfr. paragrafo 3.1.
[53] Corte di giustizia europea, sentenza del 24 novembre 2011, C-70/10, *Scarlet Extended*; sentenza del 16 febbraio 2012, C-360/10, *SABAM*. Sul punto: D'Ambrosio (2012), p. 85; Pollicino (2014), p. 634; Sammarco (2012), p. 301-303; Picotti (2012), p. 2555.
[54] Ibidem.
[55] Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Strategia per il mercato unico digitale in Europa*; COM(2015) 192 *final* del 6 maggio 2015.

3.1. *Le recenti evoluzioni in ambito europeo in materia di piattaforme online.*

Prima di indicare i nuovi interventi normativi che sono stati adottati in seno all'Unione Europea, è opportuno operare una ricostruzione delle novità che il tema della responsabilità dei gestori dei servizi in rete ha vissuto negli ultimi anni, sulla base delle diverse Comunicazioni della Commissione al Parlamento europeo e al Consiglio[56].

La prima di queste, come sopra menzionato, è quella riguardante la Strategia per un Mercato Unico Digitale europeo[57], nella quale la Commissione, conformandosi alle risultanze giurisprudenziali sul tema, ribadisce che la sola forma di responsabilità delineabile a carico di questi soggetti è una forma di responsabilità "*ex post*"[58], fondata, in virtù di un dovere di diligenza facente capo agli stessi, sulla mancata rimozione di contenuti illeciti di cui gli intermediari siano effettivamente a conoscenza.

Lo sviluppo di queste premesse ha condotto a due successive Comunicazioni[59], con le quali si è deciso di adottare un approccio settoriale in materia, privilegiando una normazione mirata su alcune questioni specifiche particolarmente sensibili e bisognose di regolamentazione, preservando invece quale base giuridica generale – in quanto ritenuta «sufficientemente flessibile»[60] – la disciplina delineata dalla direttiva del 2000 sul commercio elettronico[61].

Sono state individuate dalla Commissione europea quattro differenti aree di intervento, alle quali hanno fatto seguito altrettante proposte di provvedimenti normativi. La prima riguarda la proliferazione di piattaforme di condivisione di video *online* con contenuti nocivi per minori e istigazioni all'odio, alla quale ha fatto seguito la direttiva sui servizi di media audiovisivi 2018/1808/UE[62]; la seconda riguarda l'utilizzo *online* di contenuti protetti dal diritto d'autore, alla quale ha fatto seguito una nuova direttiva in materia di diritto d'autore[63]; la terza concerne la lotta contro gli abusi sessuali sui minori e la pedopornografia *online*, rispetto alla quale vi è già la direttiva 2011/93/UE[64]; e infine l'ultima area di intervento è rappresentata dalla lotta al *cyber*-terrorismo, cui ha fatto seguito dapprima la direttiva 2017/541/UE[65] e, successivamente, la proposta di Regolamento relativo alla prevenzione della diffusione di contenuti terroristici *online*[66].

In tutte le fonti sopra elencate sono presenti disposizioni che contemplano, direttamente a carico degli ISP o per il tramite dei prossimi interventi nazionali, obblighi giuridici di diverso contenuto e portata. Brevemente, le direttive in materia di contrasto alla pedopornografia ed al terrorismo in rete impongono agli Stati membri di adottare le «*misure necessarie*», senza che queste vengano meglio articolate o spiegate, per assicurare la tempestiva rimozione di pagine web o contenuti *online* che, rispettivamente, consistano in materiale pedopornografico o in pubblica provocazione a commettere un reato di terrorismo, come delineato dall'art. 5 della direttiva 541/2017[67].

[56] Per una esaustiva esposizione sul tema cfr. Montagnani (2018).
[57] Comunicazione della Commissione, *Strategia per il mercato,* cit.
[58] L'ipotesi di una responsabilità *ex ante* è stata esclusa dalla giurisprudenza: Corte di giustizia europea, sentenza del 24 novembre 2011, C-70/10, *Scarlet Extended*, EU:C:2011:771; sentenza del 16 febbraio 2012, C-360/10, *SABAM*, EU:C:2012:85; nella giurisprudenza nazionale basti richiamare il noto caso Google c. ViviDown, Cass. Pen., Sez. III, 17 dicembre 2013, n. 5107, in *Dir. fam.*, 2014, 2, p. 675 ss.
[59] Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Le piattaforme* online *e il mercato unico digitale. Opportunità e sfide per l'Europa,* COM(2016)288 *final;* Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Lotta di contenuti illeciti* online. *Verso una maggiore responsabilizzazione delle piattaforme* online, COM(2017)555 *final.*
[60] Nordemann (2017)*:* documento preparato per il *Policy Department* A su richiesta della commissione del Parlamento europeo per il mercato interno e la protezione dei consumatori del Parlamento europeo, 2017, disponibile al sito http://www.europarl.europa.eu.
[61] In questo senso la Commissione nella Comunicazione del 2016: «la Commissione manterrà l'attuale regime di responsabilità relativo agli intermediari, adottando al contempo un approccio di regolamentazione di tipo settoriale».
[62] Direttiva 2018/1808/UE del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato.
[63] Direttiva 2019/790/UE del Parlamento Europeo e del Consiglio del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE.
[64] Direttiva 2011/92/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio.
[65] Direttiva 2017/541/UE del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio.
[66] COM(2018) 640 *final,* nella sua ultima versione approvata a seguito della discussione al Consiglio del 22 maggio 2019.
[67] Art. 25 direttiva 2011/92/UE e art. 21 direttiva 2017/541/UE.

Scende più nel dettaglio la proposta di Regolamento per la prevenzione della diffusione di contenuti terroristici *online*, che coinvolge i prestatori di servizi di *hosting* su diversi fronti. Infatti, essi: (i) laddove siano a conoscenza o siano consapevoli dell'esistenza di contenuti terroristici nei loro servizi, dovranno informare le autorità competenti ed eliminare tali contenuti rapidamente; (ii) dovranno rimuovere i contenuti terroristici o disabilitarne l'accesso il prima possibile, e in ogni caso entro un'ora dal ricevimento di un ordine di rimozione ricevuto dalla competente autorità; (iii) potranno adottare «*misure specifiche*», efficaci, mirate e proporzionate per proteggere i loro servizi dalla diffusione pubblica di contenuti terroristici; (iv) infine dovranno predisporre «*misure di salvaguardia efficaci e appropriate per garantire l'accuratezza e la fondatezza delle decisioni*» di rimozione di contenuti ritenuti terroristici fondate su strumenti automatizzati, misure che consistono in particolare nella previsione di una sorveglianza umana e di meccanismi di verifica dell'adeguatezza della decisione di rimuovere un contenuto o di negarvi l'accesso.

Non altrettanto articolata è la disciplina prevista dalla direttiva in materia di servizi di media audiovisivi, il cui art. 1 introduce l'art. 28 *ter* nella direttiva 2010/13[68], ai sensi del quale gli Stati membri dovranno assicurare, in sede di attuazione, l'adozione – da parte dei fornitori di servizi – di «*misure adeguate*»[69], praticabili e proporzionate, «*per tutelare*» i minori nonché il grande pubblico da contenuti nocivi, che istighino alla violenza e all'odio, ovvero contenuti la cui diffusione integri una fattispecie di reato ai sensi del diritto dell'Unione Europea.

Per quanto riguarda, infine, la direttiva in materia di diritto d'autore, assume importante rilievo la formulazione del molto discusso articolo 13, il quale prevedeva inizialmente – nella versione elaborata dalla Commissione – l'obbligo a carico dei prestatori di servizi, che memorizzano e danno pubblico accesso a grandi quantità di opere o altro materiale caricato dagli utenti, di adottare misure «*volte ad impedire*» che il materiale identificato dai titolari dei diritti fosse messo a disposizione sui propri servizi. Il testo di questo articolo, criticato sotto diversi aspetti, in particolare perché aggravava considerevolmente la posizione dei *provider* e non si coordinava con la disciplina della direttiva *e-commerce*[70], è stato successivamente modificato, per poi diventare l'art. 17 della direttiva approvata.

Tale norma dispone, in primo luogo, al paragrafo 4, che il *provider* che abbia agito in assenza d'autorizzazione dei titolari dei diritti d'autore[71] sia ritenuto responsabile, a meno che non dimostri di: (a) aver fatto il possibile per ottenere l'autorizzazione; (b) aver fatto il possibile, conformemente agli elevati standard industriali di diligenza professionale, per assicurare l'indisponibilità di materiale protetto dal diritto d'autore per il quale i titolari abbiano fornito all'intermediario sufficienti e necessarie informazioni; (c) aver, in ogni caso, agito speditamente, una volta ricevuta una notifica sufficientemente motivata da parte del titolare di diritti, rimuovendo o disabilitando l'accesso al contenuto segnalato, facendo il possibile per prevenire futuri caricamenti di quello stesso contenuto. Nel successivo paragrafo, inoltre, il nuovo testo dell'art. 17 descrive alcuni dei criteri[72] che devono essere tenuti in considerazione nella valutazione delle misure che permettono ai *provider* di andare esenti da responsabilità. È da specificare, infine, che nel sesto paragrafo viene previsto un regime diversificato sulla base della dimensione del *provider*. Infatti, i *content sharing service provider* che prestano servizi nell'Unione Europea da meno di 3 anni e con fatturato annuale sotto i 10 milioni di Euro, per andare esenti da responsabilità, dovranno dimostrare solamente di: (a) aver fatto il possibile per ottenere l'autorizzazione, (b) aver agito speditamente, una volta ricevuta una notifica sufficientemente motivata da parte del titolare di diritti, rimuovendo o disabilitando l'accesso

[68] Direttiva 2010/13/UE del Parlamento europeo e del Consiglio relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi).

[69] Misure che devono essere predisposte in base ai seguenti criteri: natura del contenuto illecito; danno che questo può provocare; categoria dei destinatari che le misure mirano a tutelare; i diversi diritti coinvolti; le dimensioni della piattaforma per la condivisione di video; la natura del servizio offerto dalla piattaforma; infine le misure non possono condurre a forme di controllo *ex ante* o filtraggio dei contenuti nel momento in cui vengono caricati.

[70] Montagnani (2018), pp. 192-198; Colangelo e Maggiolino, (2018), pp. 142-159; Colangelo e Torti (2019), pp. 75-90; Van Vegchel (2018), pp. 1-9.

[71] Secondo quanto previsto dall'art. 3 della direttiva 2001/29/UE (direttiva sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione), la quale dispone che: «*gli Stati membri riconoscono agli autori il diritto esclusivo di autorizzare o vietare qualsiasi comunicazione al pubblico, su filo o senza filo, delle loro opere, compresa la messa a disposizione del pubblico delle loro opere in maniera tale che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente*».

[72] Tra gli altri: la tipologia, il pubblico e la dimensione del servizio e la tipologia di opere o altri materiali caricati dagli utenti del servizio; la disponibilità di strumenti adeguati ed efficaci e il relativo costo per i prestatori di servizi.

al contenuto segnalato. Mentre i *service provider* con un numero medio di visitatori mensili di più di 5 milioni (calcolato sulla base dell'anno precedente) dovranno dimostrare anche di aver fatto il possibile per prevenire *futuri* caricamenti del contenuto segnalato.

Una simile formulazione dell'art. 17, che, da una parte, prevede obblighi "attivi" incidenti direttamente sui contenuti ospitati a carico dei *provider* – senza quindi più delegare ad accordi di licenza tra privati il compito di regolamentare le responsabilità in materia –, e, dall'altra, pur utilizzando generiche locuzioni quali «*assicurare l'indisponibilità*», «*agire per rimuovere*» o «*prevenire futuri caricamenti*», cerca di specificare e descrivere maggiormente nel dettaglio l'apparato degli obblighi a carico degli ISP, sembra rappresentare una soluzione più equilibrata, che contempera le diverse istanze soggettive alla stregua di parametri oggettivi.

Si nota in ogni caso una chiara evoluzione tra le più risalenti e le più recenti proposte: dall'utilizzo di formule ampie quali «*misure necessarie*» o «*misure adeguate*», la cui predisposizione ed articolazione sarebbe stata rimessa agli Stati membri, o addirittura ad accordi privati, si sta passando a norme, aventi quali destinatari direttamente i *provider,* che delineano in modo più preciso e dettagliato le misure che è necessario adottino per essere esentati da responsabilità.

Benché dunque l'approccio che le istituzioni europee hanno deciso di adottare sia di tipo settoriale, si evince una linea che accomuna i diversi interventi in materia di responsabilità per la gestione delle piattaforme *online* a livello europeo: l'attenzione viene concentrata sulla necessità di interventi di rimozione, da parte degli intermediari, di contenuti lesivi di interessi e posizioni soggettive giuridicamente rilevanti, con un'urgenza ed un'incisività delle misure che cresce proporzionalmente alla gravità del contenuto illecito, parametrata alla gerarchia dei beni giuridici offesi.

Dal quadro delineato, integrato dalle diverse pronunce giurisprudenziali[73], emerge quindi come ormai consolidata l'esigenza di una maggior responsabilizzazione dei prestatori di servizi in rete[74], in virtù del fondamentale ruolo che essi possono svolgere nel contrasto ai fenomeni criminosi nel *Cyberspace*[75]. E tale esigenza, che trova diversi riscontri anche nello scenario nazionale[76], sarà almeno in parte soddisfatta dalle future norme europee e dalla loro attuazione.

4. La configurabilità di una responsabilità penale ex post in capo agli ISP.

Perché si possa prevedere una responsabilità penale dell'intermediario per omessa rimozione di un contenuto illecito il cui caricamento da parte di un utente costituisce reato, occorre risolvere in prima istanza il nodo problematico relativo alla sussistenza di una posizione di garanzia in capo a questi soggetti.

In merito a questo problema, quella parte di dottrina che non ritiene individuabile in capo agli ISP un obbligo di impedimento dei reati commessi dai propri utenti, non lo ritiene sussistente nemmeno in questa seconda fase. Ai sensi della normativa vigente, vi sarebbero in capo agli ISP (e più precisamente agli *hosting provider*) solamente due obblighi: un mero obbligo di *notice,* «ossia di informazione dell'autorità competente del carattere illecito del contenuto del servizio ospitato»[77], ed un obbligo di *take down,* «ossia di rimozione del dato su richiesta

[73] Cfr. nota n. 29.

[74] Circostanza confermata anche dalla Relazione del Parlamento europeo sulle piattaforme *online* e il mercato unico digitale del 31 maggio 2017, A8-0204/2017; nonché dalla Raccomandazione (UE)2018/334 della Commissione del 1° marzo 2018 sulle misure per contrastare efficacemente i contenuti illegali *online*.

[75] Secondo Andrew Shapiro «in democratic societies, those who control the access to information have a responsibility to support the public interest. (…) these gatekeepers must assume an obligation as trustees of the greater good»: cfr. Shapiro (2000), p. 225 così come riportato da Frosio (2018), p. 7.

[76] All'interno della legislazione italiana assumono particolare rilevanza, oltre all'art. 16 D.lgs. n. 70/2003, attuativo della direttiva sull'*e-commerce*, anche gli artt. 14 *ter* e 14 *quater* L. n. 269/1998, introdotti dalla L. n. 38/2006 in attuazione della decisione del Consiglio dell'Unione europea del 29 giugno 2000 relativa alla lotta contro la pedopornografia infantile in Internet, i quali impongono a carico dei fornitori di servizi obblighi di segnalazione di materiale pedopornografico e di filtraggio di siti segnalati dall'organismo competente, senza tuttavia toccare procedure o obblighi di rimozione (sul punto cfr. Torre (2013), pp. 163-191). Così come è da ricordare l'art. 2 c. 3 e 4 del d.l. n. 7/2015, secondo il quale i fornitori di connettività e di servizi in rete hanno l'obbligo, rispettivamente, di inibire l'accesso a siti contenenti materiale terroristico o di rimuovere (entro 48 ore) contenuti terroristici, sempre a seguito di un ordine dell'autorità.

[77] Manna e Di Florio (2019), p. 913.

dell'autorità competente»[78]; ma né l'uno né l'altro potrebbero essere considerati quali fonte di una posizione di garanzia.

Tuttavia, è da sottolineare che, seppur la questione rimanga controversa anche in giurisprudenza[79], in una recente sentenza[80] la Cassazione ha statuito che l'*hosting provider*, di fronte ad una situazione di illiceità "manifesta" dell'altrui condotta, di cui non ne ha impedito la protrazione, mediante la rimozione delle informazioni o la disabilitazione all'accesso, risponderà per fatto proprio colpevole, essendogli rimproverabile una responsabilità commissiva mediante omissione, per avere concorso nel comportamento lesivo altrui. Ed una tale ricostruzione è resa possibile in virtù del fatto che «l'art. 16 d.lgs. n. 70 del 2003 fonda una cd. posizione di garanzia dell'*hosting provider*, che, se per definizione è indispensabile alla stessa originaria perpetrazione dell'illecito del destinatario del servizio, ne diviene giuridicamente responsabile solo dal momento in cui gli possa essere rimproverata l'inerzia nell'impedirne la protrazione»[81].

Muovendo da queste recenti evoluzioni, è inoltre da evidenziare come, secondo una parte minoritaria della dottrina[82], vi siano da tempo disposizioni normative extra-penali che prevedono obblighi specifici in capo agli ISP in materia di reati di diffusione di materiale pedopornografico, in materia di violazioni di diritto d'autore e nello stesso D.lgs. n. 70/2003, capaci di integrare in capo al prestatore di servizi una responsabilità penale per reato omissivo improprio.

Guardando quindi alle novità in ambito europeo, agli sviluppi giurisprudenziali sopra richiamati, uniformemente orientati verso una maggior responsabilizzazione dei prestatori di servizi in rete, nonché alle nuove discipline normative che stanno delineandosi in seno alle istituzioni europee, le quali prefigurano «obblighi giuridici derivanti dal diritto dell'UE e nazionale»[83] ed un «dovere di diligenza»[84] nell'esercizio delle predette attività, non sembra più poter escludersi, in capo agli intermediari, la configurabilità di obblighi giuridicamente rilevanti di attivarsi per impedire reati.

Gli *hosting provider* infatti, in virtù della posizione di "signoria" che rivestono nei confronti dei dati trattati sulle proprie piattaforme[85], «(…) hanno la pesante responsabilità, nei confronti della società, di proteggere gli utenti e il pubblico in generale, nonché prevenire lo sfruttamento dei loro servizi da parte di criminali e altri soggetti coinvolti in attività illegali *online*»[86]. Guardando in effetti al contenuto sostanziale, prima ancora che formale, dell'obbligo giuridico di impedimento, esso trova valido fondamento nello stesso dato di fatto che le vittime del crimine cibernetico – in particolare quando si tratta di reati che si consumano interamente nel *Cyberspace* – si trovano nell'impossibilità di proteggere il bene giuridico leso, dato che un utente non ha possibilità di rimuovere un contenuto illecito una volta che questo è immesso in rete.

Inoltre, la dimensione sociale che ha assunto il *Cyberspace,* strumento attraverso cui si esercitano i più diversi diritti anche fondamentali[87], fa assumere al suo corretto e buon utilizzo il valore di interesse diffuso, la cui tutela può costituire ulteriore ragione per il ricorso

[78] Ibidem.
[79] La V sezione penale della Corte di Cassazione non ha ritenuto configurabile una posizione di garanzia in capo agli ISP in una recente sentenza, la n. 12546 del 20 marzo 2019, (in *Diritto di Internet,* 2019, 3, p. 575 ss.). Di avviso opposto sono invece: Cass. Pen., sez. V, 27 dicembre 2016, n. 54946, in *Foro it.*, 2017, p. 251 ss.; Cass. civ., sez. I, 19 marzo 2019, n. 7708, in *Dir. inf.*, 2019, 1, p.152 ss. e in *Foro it.,* 2019, 6, I, p. 2045 ss., con nota di Di Ciommo, *Oltre la direttiva 2000/31/CEE, o forse no. La responsabilità dei* provider *di Internet nell'incerta giurisprudenza europea.*
[80] Cass. civ., sez. I, 19 marzo 2019, n. 7708, cit.
[81] Ibidem.
[82] Picotti (1999), pp. 504-506; Picotti (2007), pp. 1207-1208; Flor (2010), pp. 457-460; Flor (2012), pp. 662-693; Torre (2013), pp. 183-191.
[83] Comunicazione della Commissione, *Lotta di contenuti illeciti,* cit., p. 7.
[84] Ibidem.
[85] In base ai dettami della c.d. teoria funzionale, il vincolo che legherebbe il comportamento doveroso dell'ISP sarebbe accompagnato da una situazione di fatto ad esso corrispondente, la quale è caratterizzata da un potere, un dominio, nei confronti del processo di produzione dell'evento dannoso che deriva da un potere di organizzazione o disposizione fondante un relativo obbligo di controllo. Tra i fondamentali riferimenti dottrinali sul punto si richiamano: Sgubbi (1975); Fiandaca (1979); Fiandaca (1983), cc. 27-45; Grasso (1983); Romano (1995), pp. 337-366; Bisori (1997), pp. 1339-1394; Leoncini (1999).
[86] Comunicazione della Commissione, *Lotta di contenuti illeciti,* cit., p. 2. Ai prestatori di servizi in rete, proprio in ragione del significato sociale e culturale che il *Cyberspace* sta assumendo, è quindi riconosciuto un preciso *ruolo economico e sociale*, il quale costituisce spinta per le istituzioni pubbliche, anche europee, all'elaborazione di obblighi positivi di condotta in virtù di quella che è ancora una vocazione solidaristica del potere pubblico.
[87] Il *Cyberspace* ha infatti prodotto «una espansione e diversificazione dei beni giuridici meritevoli di tutela penale»: tra questi basti menzionare la riservatezza informatica nonché la *privacy* in senso stretto. Sul punto cfr. Picotti (2019), p. 52; Picotti (2004), pp. 21-95.

al meccanismo proprio delle fattispecie omissive improprie[88]. L'attivazione della clausola di equivalenza sarebbe per di più legittimata nei casi in cui i beni giuridici oggetto di tutela siano di rango primario, come quelli offesi dalla pedopornografia *online*[89].

Passando al profilo formale, l'attribuzione di una posizione di garanzia in capo agli ISP può trovare riscontro, come già rilevato, nella previsione di obblighi giuridici aventi fonte normativa, primo fra tutti quello delineato, per gli *hosting provider,* dall'art. 16 c. 1 D.lgs. n. 70/2003[90], il quale, tuttavia, andrebbe, oltre che meglio articolato, ritenuto applicabile a tutti gli *hosting provider*.

Secondo un orientamento giurisprudenziale alquanto consolidato[91], infatti, il regime delineato dalla direttiva *e-commerce*, al cui considerando 42 specifica come «*le deroghe alla responsabilità stabilita nella presente direttiva riguardano esclusivamente il caso in cui l'attività di prestatore di servizi (…) sia di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore non conosce né controlla le informazioni trasmesse o memorizzate*», non sarebbe applicabile ai c.d. *hosting* attivi. Si tratta di quegli intermediari che completano ed arricchiscono con un qualche apporto la fruizione dei contenuti da parte degli utenti[92], elementi idonei a delineare la figura di *hosting provider* attivo, o "indici di interferenza" – da accertare in concreto –, sono, ad esempio, «le attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione»[93].

Il persistere su questa posizione conduce, tuttavia, a diversi rischi, dovuti al fatto che la stessa distinzione tra *hosting* attivi e passivi comincia a rivelarsi non sufficientemente efficace. Il prevedere infatti, da una parte, obblighi aventi ad oggetto misure incidenti (sia in termini di rimozione, che di filtraggio) sulle informazioni ospitate dai *provider* e il sostenere, dall'altra, che il regime di esenzione da responsabilità non sia applicabile ai c.d. *hosting* attivi, conduce ad una contraddizione, poiché vi è il rischio che gli stessi obblighi previsti a carico degli ISP rendano quest'ultimi "attivi"[94].

Inoltre, la distinzione tra *hosting* attivi e passivi rivela la propria inadeguatezza se si considera la variabilità a cui è soggetto il parametro dell'attività posta in essere dai singoli intermediari, dal momento che la stessa, strettamente legata all'incessante e veloce sviluppo tecnologico, è in costante e repentino mutamento ed adeguamento[95]. Ancorare una categorizzazione ad un parametro instabile comporta innumerevoli rischi. Pertanto, come è stato sostenuto in dottrina[96], il criterio di valutazione delle responsabilità dovrebbe spostarsi dal campo della soggettività a quello dell'oggettività, non considerando (esclusivamente) le posizioni che soggettivamente assumono i prestatori in virtù delle attività poste in essere – le quali, peraltro, risultano oggi essere per la maggior parte segnate da caratteri "attivi", non esistendo più attività

[88] Ritornando utili e ancora attuali le parole di Giovanni Fiandaca, il quale, riferendosi alla tutela dell'ambiente e della salute del consumatore, sostiene che si tratti di tutelare beni primari «che risultano più esposti alle potenzialità lesive di un sistema produttivo di massa tecnologicamente sempre più complesso ma non altrettanto attrezzato nella prevenzione dei danni». E ancora: «una più efficace difesa contro la moderna fenomenologia dannosa richiede un controllo dell'attività produttiva che finisce con l'incidere in senso restrittivo sul conseguimento di un profitto d'impresa tendenzialmente illimitato», in Fiandaca (1979), p. 56.

[89] D'Ambrosio (2012), pp. 79-81.

[90] Secondo il quale: «*Nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso*». Oltre agli obblighi di rimozione che stanno nascendo all'interno delle discipline di settore sopra esaminate. Nell'ordinamento nazionale il riferimento va inoltre; agli artt. 14 *ter* e *quater* L. n. 269/1998 (su cui cfr. Picotti (2007), pp. 1196-1211; Salvadori (2007), pp. 1074-1075); nonché agli artt. 156, 156 bis e 163 L. n. 633/1941 (su cui cfr. Flor (2010), pp. 457-460).

[91] Per la giurisprudenza europea cfr. nota n. 20. Nella giurisprudenza nazionale: Corte di Appello di Milano, 7 gennaio 2015, n. 29, in *Dir. Industriale*, 2015, 5, p. 455 ss. con nota di Marvasi; Tribunale di Torino, 07 aprile 2017, n. 1928, in *Diritto & Giustizia*, 3 luglio 2017; Corte d'Appello di Roma, 28 aprile 2017, n. 2833, inedita.

[92] Così come definiti da ultimo da Cass. civ., sez. I, 19 marzo 2019, n. 7708, cit.

[93] Ibidem.

[94] Dove con "attivi" si intendono, secondo quanto si evince dalla giurisprudenza europea (cfr. nota n. 19), quei prestatori di servizi che eseguono attività che gli permettono di controllare o conoscere le informazioni trasmesse o memorizzate, come le attività di posizionamento, indicizzazione ed organizzazione dei contenuti.

[95] In dottrina è stato proposto di ancorare la valutazione giuridica dei fenomeni ad una nuova componente: la "variabile tecnologica", di modo che l'organo giudicante o le parti, nel soddisfare i propri oneri probatori, possano dare una lettura giuridica della situazione coinvolgente le piattaforme sulla base delle tecnologie che esse avevano a disposizione: Piraino (2017), p. 153.

[96] Ivi, p. 197.

di *hosting* autenticamente e meramente passive[97] –, ma concentrando l'attenzione invece sulle «fattispecie concrete nelle quali gli intermediari sono a conoscenza, o avrebbero potuto essere a conoscenza, adottando la diligenza professionale, di elementi di fatto che rivelano in modo manifesto la commissione di un illecito da parte di loro utenti»[98].

Per quanto riguarda l'elemento soggettivo, l'art. 16 D.lgs. 70/2003 richiede che vi sia in capo all'*hosting provider* l'«*effettiva conoscenza*» del contenuto illecito, la quale quindi dovrà tradursi in termini di dolo diretto (escludendosi il dolo eventuale in virtù dell'inciso "*effettiva*"[99]) e, in particolare, in termini di dolo di partecipazione, se si tratti di concorso omissivo nel reato commissivo dell'utente. Anche l'elemento soggettivo risentirà tuttavia dei più recenti sviluppi nella materia. Infatti, da una parte, le nuove attività poste in essere dagli *hosting provider*, caratterizzati dall'esercizio di operazioni sui dati a volte invasive, nonché da maggiori capacità di monitoraggio, analisi e controllo, forniscono al giudice importanti indici sintomatici per l'accertamento dell'elemento soggettivo[100]. Dall'altra parte, la partecipazione attiva degli utenti potrebbe influenzare l'oggetto dello stesso: ad esempio, difficilmente si potrebbe richiedere, ai fini dell'integrazione dell'elemento soggettivo, che il *provider* conosca l'identità del singolo utente che ha caricato il contenuto illecito integrante reato[101].

In conclusione, l'obbligo di impedimento del reato, la cui omissione potrebbe fondare una responsabilità del *provider*, si articolerebbe sulla base del sistema di responsabilità *ex post* fondato sul binomio effettiva conoscenza-mancata rimozione[102], il cui contenuto si potrà ricavare o dalla futura attuazione delle singole norme europee di settore sopra riportate, ovvero da quelle già esistenti, o, infine, dal generale obbligo di rimozione ex art. 16 D.lgs. n. 70/2003, il cui contenuto andrebbe tuttavia meglio articolato.

4.1. *Una disciplina non al passo coi tempi.*

La decisione di non intervenire sulla direttiva *e-commerce* rappresenta un'occasione mancata per dare certezza, coerenza e uniformità alla disciplina della responsabilità dei prestatori di servizi in rete. Benché un approccio settoriale presenti indiscussi i vantaggi – e risulti irrinunciabile data la complessità e diversità delle attività e dei contenuti presenti in rete –, una maggior articolazione della base giuridica comune alle singole materie sembra essere quanto meno opportuna.

La direttiva del 2000 è stata infatti definita da più voci[103] come inadeguata e non più attuale. Il rischio quindi di elaborare dettagliati interventi in settori particolarmente sensibili, mantenendo la direttiva del 2000 quale base normativa comune, in quanto sufficientemente elastica e ampia, è quello di creare uno scenario a macchia di leopardo, in cui vi sono settori dettagliatamente regolamentati ed altri affidati alla discrezionalità dei soggetti privati che vi operano. Una simile deriva priverebbe la regolamentazione delle comunicazioni in Internet di una logica unitaria e di sistema, pretesa invece «dal carattere a-territoriale della rete»[104].

Si possono schematicamente riscontrare due differenti lacune nel regime delineato dagli artt. 12 ss. della direttiva 31/2000: (i) vi è un mancato adeguamento delle diverse definizioni degli ISP, i quali vanno distinti, utilizzando criteri elastici capaci di adeguarsi allo sviluppo tecnologico, sulla base sia delle diverse attività, sia della loro dimensione – in termini di quantità di dati processati, nonché di numero di utenti; (ii) si rende opportuna una maggiore articolazione e specificazione del regime di responsabilità di cui all'art. 14 della direttiva – sulla scorta dei modelli riscontrabili nelle direttive e proposte di direttive sopra esaminate.

[97] Cfr. paragrafo 2 sulle evoluzioni degli strumenti tecnologici a disposizione delle piattaforme.
[98] Piraino (2017), p. 198.
[99] Seminara (1998), p. 101; Flor (2010), p. 463.
[100] D'Ambrosio (2012), pp. 67-93.
[101] In questo senso Cass. Pen., Sez. V, 11 dicembre 2017, n. 13398, in *Foro it.*, 2018, 5, 2, cc. 305-309.
[102] Questo punto dovrebbe essere arricchito da una riflessione sulla portata dell'inciso «*su comunicazione delle autorità competenti*» presente nel testo dell'art. 16 c. 1 lett. b) D.lgs. n. 70/2003, che non è possibile articolare per ragioni di brevità. Sulla natura "superflua" di questo inciso si segnalano in ogni caso: Tribunale civile di Torino, 7 aprile 2017, n. 1928, in *Danno resp.*, 2018, 1, p. 87 ss.; Tribunale civile di Napoli Nord, 3 novembre 2016, in *Giur. it.*, 2017, 3, p. 629 ss.; Cass. Pen., Sez. V, 27 dicembre 2016, n. 54946, in *Foro it.*, 2017, p. 251 ss.; Corte d'Appello di Milano, 7 gennaio 2015, in *Dir. ind.*, 2015, 5, p. 455 ss.; Tribunale di Roma, 22 gennaio 2010, inedita; Tribunale di Trani, 14 ottobre 2008, in *Danno resp.*, 2009, 1059.
[103] Cfr. nota n. 18.
[104] Petruso (2018), pp. 511-558.

Per quanto riguarda l'art. 14 della direttiva del 2000, le due condizioni d'esenzione delineate andrebbero maggiormente articolate e specificate. Ai sensi della lettera a) (prima condizione), l'ISP deve restare esente da responsabilità se non è «*effettivamente a conoscenza*» del contenuto illecito o di «*fatti o di circostanze che rendono manifesta l'illegalità*» del contenuto. Tale requisito dovrebbe essere rivisto alla luce delle interpretazioni della Corte di Giustizia europea, secondo la quale l'ISP è «effettivamente a conoscenza»[105] quando «viene ad essere, in qualunque modo – sia attraverso la segnalazione da parte di terzi *sia attraverso un esame effettuato di propria iniziativa* –, al corrente di fatti o circostanze in base ai quali un operatore economico diligente[106] avrebbe dovuto constatare l'illiceità dei contenuti dalla stessa ospitati»[107].

Ai sensi della lettera b) dell'art. 14 della direttiva 31/2000 (seconda condizione d'esenzione), l'ISP deve restare esente da responsabilità se, «*non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso*». Per quanto riguarda tale ipotesi, la rimozione dovrebbe inserirsi all'interno di un meccanismo attraverso il quale sia più semplice provarne, a seconda dei casi, l'eventuale omissione ed il grado di esigibilità. La formalizzazione di un meccanismo generale di *notice and take/stay down* – non limitato a singoli settori – potrebbe garantire un grado di certezza e di tutela sufficienti. Una tale regolamentazione costituirebbe uno strumento adeguato per un equilibrato contemperamento dei diritti ed interessi dei soggetti interessati[108], nonché eviterebbe agli ISP di assumere il ruolo di censori della rete, con prerogative che sono piuttosto di carattere prettamente pubblicistico.

Partendo dal modello offerto dalla legislazione tedesca con il c.d. *Facebook Act,* in vigore dal 1° ottobre 2017[109], ed accogliendo un orientamento riscontrabile in seno alla Corte europea dei diritti dell'uomo[110], la predisposizione di un meccanismo unico – applicabile quindi in ogni settore – di *notice and take down,* articolato attraverso una diversificazione degli obblighi di rimozione in base al grado di illiceità che il contenuto manifesta, potrebbe orientare un adeguato e uniforme sistema di tutele.

Il pregio di un modello fondato su questo parametro è quello di articolarsi attraverso il coinvolgimento di tutte e tre le soggettività che operano nel *Cyberspace*: coinvolge gli utenti, i quali saranno responsabilizzati attraverso il compito di fornire segnalazioni informate e dettagliate; coinvolge i *provider*, sui quali ricadono i maggiori oneri e obblighi; coinvolge le autorità pubbliche, a cui gli utenti possono rivolgersi e con le quali gli operatori instaurano continui flussi comunicativi per la risoluzione dei casi più problematici.

Vi sono infatti, da un lato, casi in cui determinati contenuti richiedono una diversa quantità di informazioni contestuali, al fine di determinarne la liceità o meno (ad esempio nei casi dubbi di diffamazione o di violazione dei diritti d'autore)[111]: ed in questi casi – prendendo ad esempio la legge tedesca[112] – l'intermediario dovrebbe poter contare sull'intervento delle autorità competenti aventi le prerogative necessarie. Dall'altro lato, vi sono invece ipotesi di contenuti manifestatamente e gravemente illeciti (ad esempio nei casi di contenuti aventi carattere terroristico) la cui rapida od anzi immediata rimozione è particolarmente importante.

Parallelamente, le procedure di cancellazione o sospensione potranno essere completa-

[105] Tradizionalmente si richiama il concetto di *actual knowledge* derivante dal DMCA (cfr. nota n. 76), con il quale si intende in modo univoco un dato cognitivo effettivo cui non può essere equiparata la conoscibilità, neppure se qualificata dalla conoscenza di particolari circostanze: in questo senso De Cata (2010), pp. 99-129.

[106] La cui diligenza andrebbe valutata sulla base dell'adozione dei meccanismi di filtraggio e rimozione di cui l'ISP era nella disponibilità, meccanismi e obblighi che tuttavia andrebbero maggiormente specificati e formalizzati.

[107] Corte di giustizia europea, sentenza del 12 luglio 2011, C-324/09, *L'Oréal,* punti 120 e 121.

[108] Come sottolineato dalla stessa Corte europea dei diritti dell'uomo nelle sentenze: *Magyar Tartalomszolgáltatók Egyesülete and Index.HU ZRT v. Hungary,* ricorso n. 22947/13, sentenza del 2/02/2016; *Delfi AS v. Estonia,* ricorso n. 64569/09, sentenza del 16/06/2015. Sul punto cfr. Falconi (2016), pp. 235-254.

[109] Cfr. nota n. 62.

[110] Corte dei diritti dell'uomo, *Pihl v. Sweden,* ricorso n. 74742/14, sentenza del 9/03/2017; *Magyar Tartalomszolgáltatók Egyesülete and Index.HU ZRT v. Hungary,* ricorso n. 22947/13, sentenza del 2/02/2016; *Delfi AS v. Estonia,* ricorso n. 64569/09, sentenza del 16/06/2015. La differenza delle soluzioni adottate nelle diverse sentenze è dovuta proprio al «principale discrimine della diversa natura dei commenti incriminati», Falconi (2016), p. 251. In dottrina cfr. anche Petruso (2018), pp. 511-558, secondo il quale «si potrebbe pensare che la Corte EDU segnali, sia pure indirettamente, la necessità di un ripensamento delle regole di responsabilità degli intermediari della rete di matrice unitario-europea da incanalarsi non più verso un principio generale, ma verso regole di volta in volta enucleabili in relazione agli specifici contenuti presenti in linea, al loro disvalore, alla loro idoneità a limitare altri diritti fondamentali di pari rango».

[111] Cfr. montagnani e Trapova (2018), p. 304, secondo cui «è altamente dubbio che qualsiasi sistema di filtraggio attualmente in uso, costoso o poco costoso, sia abbastanza sofisticato per tracciare in modo sufficientemente adeguato la linea tra una parodia e un uso illecito o una qualsiasi delle altre eccezioni previste dall'articolo 5 della direttiva 2001/29/CE e nelle diverse leggi sui diritti d'autore degli Stati membri».

[112] Ai sensi del § 3 comma 2 della *NetzDG* tedesca l'ISP può rimettere, entro sette giorni, la decisione sulla natura illecita di un contenuto ad un organo di autoregolamentazione, accreditato da un'autorità amministrativa competente.

mente automatizzate e autonome solo quando non vi siano dubbi sull'illiceità dei contenuti (come accade nel caso di contenuti terroristici e di incitamento al terrorismo)[113]; mentre nei casi di illiceità meno manifesta, si dovrà ricorrere a procedure non completamente automatiche ma contemperate da correttivi, quali l'analisi dei casi controversi da parte di operatori interni all'intermediario nonché la collaborazione con organismi esterni e pubblici aventi le competenze giuridiche, oltre che tecniche, necessarie per definire un contenuto quale illecito.

Ulteriori correttivi, ricavabili dalla giurisprudenza della Corte di giustizia europea[114] e già peraltro utilizzati dalla giurisprudenza nazionale[115], potrebbero consistere, da una parte, nella possibilità lasciata agli intermediari di scegliere le specifiche misure tecniche concrete, attraverso cui conformarsi all'obbligo, secondo quelle che sono le proprie capacità; dall'altra parte, nel concedere l'esenzione da responsabilità all'ISP che dimostri di aver adottato tutte le misure ragionevoli, in quanto mirate ed efficaci alla rimozione dei contenuti illeciti, e che garantiscano la possibilità agli utenti di accedere in modo lecito alle informazioni disponibili a loro destinate.

È opportuno considerare tuttavia che la distinzione fondata sulla "manifesta illeceità" dei contenuti presenti sulle piattaforme *online* potrebbe porre problemi in termini di tassatività e determinatezza. Non è infatti di semplice delimitazione il concetto di «*manifesta illiceità*»[116], il quale dovrebbe essere puntualmente definito dai legislatori attraverso tecniche di richiamo o nuove elaborazioni. Si tratta dunque di possibili evoluzioni che necessitano di ulteriori approfondimenti.

4.2. *Le problematiche poste dalla previsione di una responsabilità* ex post.

La configurabilità di una responsabilità penale dell'intermediario per la mancata rimozione di un contenuto illecito, della cui presenza sulla propria piattaforma il prestatore sia effettivamente a conoscenza, si scontra, tuttavia, con due perplessità da superare: la prima attinente a ragioni di politica criminale; la seconda alla costruzione dogmatica di questa ipotesi.

Sotto il primo profilo, il permettere di ricorrere allo strumento penale contro gli ISP per qualsiasi reato cibernetico commesso dagli utenti potrebbe condurre ad un inasprimento di quello che è stato definito il «dilemma»[117] del *provider*. Il prestatore di servizi, per tutelarsi, potrebbe infatti ricorrere ad una rimozione massiva ed indiscriminata di ogni informazione potenzialmente lesiva di diritti altrui.

La diversificazione degli obblighi (di rimozione, ma anche di filtraggio), che si è cercata di delineare nei precedenti paragrafi, sulla base del tipo e della gravità del contenuto illecito aiuterebbe ad evitare tale deriva, indirizzando e modellando gli interventi che gli operatori privati mettono in pratica in un'ottica di prevenzione e controllo[118].

Sotto il secondo profilo, non può che rilevarsi come la tenuta dogmatica di un simile sistema si fondi su un presupposto: la rimozione dell'informazione illecita da parte dell'ISP

[113] Comunicazione della Commissione, *Lotta ai contenuti illeciti*, cit., p. 15.

[114] Corte di giustizia europea, sentenza del 27 marzo 2014, *UPC Telekabel Wien*, C-314/12, EU:C:2014:192. Secondo la Corte è lecito un provvedimento inibitorio tramite il quale si vieta a un ISP di concedere ai suoi abbonati l'accesso ad un sito web che metta in rete materiali protetti senza il consenso dei titolari dei diritti, purché tale provvedimento: (i) non specifichi quali misure il *provider* deve adottare; (ii) l'*access provider* possa evitare sanzioni per la violazione di tale provvedimento attraverso la prova di aver adottato tutte le misure ragionevoli, le quali non devono privare inutilmente gli utenti di Internet della possibilità di accedere in modo lecito alle informazioni disponibili, ma devono impedire o, almeno, rendere difficilmente realizzabili le consultazioni non autorizzate dei materiali protetti e scoraggiare seriamente gli utenti di Internet che ricorrono ai servizi del *provider* dal consultare tali materiali messi a loro disposizione in violazione del diritto di proprietà intellettuale.

[115] Tribunale di Milano, Ord., 11 giugno 2018, in *Quotidiano Giuridico*, 2018.

[116] L'espressione «*contenuto manifestatamente illecito*» contenuta nel paragrafo 3 del *NetzDG* lascia, attraverso una delega in bianco, il compito valutativo a un privato: cfr. Abbondante (2017), p. 66.

[117] De Cata (2010), p. 204; Bartoli (2013), p. 606.

[118] La regolamentazione puntuale del contenuto e delle modalità di esplicazione dell'obbligo giuridico di attivarsi (in questo caso di rimozione) dell'ISP risponderebbe anche alle obiezioni che vengono sollevate dalla dottrina al sistema di responsabilità fondato sull'art. 40 cpv., secondo le quali il regime dei reati omissivi impropri rischierebbe di non rispettare pienamente il principio di legalità da una parte (quando si ricorrere alla teoria funzionale) o il principio di determinatezza dall'altra parte (quando si ricorre alla teoria formale). Per quanto riguarda le discipline normative già oggi esistenti, oltre al modello del c.d. *Facrbook Act* sopra menzionato, è opportuno richiamare l'esempio della legge italiana sul *cyber*-bullismo, L. n. 71/2017.

deve *poter impedire* l'evento o, meglio, il reato, in caso di concorso[119]. Quindi l'omissione, ossia la mancata rimozione del contenuto illecito, deve assumere il valore di contributo causale all'integrazione del reato cibernetico, poiché se così non fosse non sarebbe prospettabile una responsabilità penale dell'intermediario per la realizzazione del reato, rappresentando il suo comportamento un mero *post factum*[120].

La problematica descritta, stimolata da due pronunce della Corte di Cassazione[121], rappresenta l'occasione per una riflessione che investe la costruzione ermeneutica delle categorie penalistiche nell'ambito di una realtà sempre più segnata da processi automatizzati e autonomi. L'individuazione della consumazione dei reati, aventi quale condotta tipica la "messa a disposizione" di un contenuto in rete, nel momento della pubblicazione, sembra infatti non tener conto della complessa fenomenologia che connota i processi tecnologici ed informatici. Il trattamento automatico che segna l'informazione immessa dall'utente in rete – la quale viene "mantenuta", riprodotta, trasmessa, diffusa nel *Cyberspace* e risulta quindi permanentemente reperibile – conduce ad una protrazione, un'espansione ed eventualmente a una riproduzione (non più riconducibile alla sfera di dominio del singolo utente), non tanto degli "effetti", ma piuttosto degli stessi elementi essenziali del fatto tipico[122].

Come ha evidenziato la giurisprudenza[123], la lesione del bene giuridico protetto, in caso di reato cibernetico, non si esaurisce nell'atto della pubblicazione, ma «continua per tutto il tempo di permanenza»[124] dell'informazione in rete.

La fase successiva al caricamento di un determinato contenuto illecito in rete è infatti connotata da un'evidente portata offensiva, connessa alla circostanza che quello stesso contenuto non solo rimane potenzialmente accessibile ad un numero indeterminato di soggetti, ma il suo grado di pubblicità è suscettibile di essere altamente incrementato dalle innumerevoli occasioni e strumenti di condivisione, che permettono ad una stessa informazione di diffondersi illimitatamente in un lasso di tempo rapidissimo.

Vi è dunque una doppia dimensione da considerare. Da una parte, una volta che un determinato contenuto viene caricato nello spazio digitale, esso entra in una «eternità mediatica»[125], capace di influire fortemente, per la sua incontrollabile capacità di pubblicizzazione e diffusione, sull'esperienza dei soggetti che risultano coinvolti. Dall'altra parte, l'architettura del *Cyberspace* permette un «effetto moltiplicatore del messaggio»[126], che, se può essere un beneficio in termini di capacità informativa, conduce inevitabilmente, quando quel messaggio ha carattere illecito, a una moltiplicazione delle potenzialità del danno, rendendo sempre più difficoltosa l'individuazione dei potenzialmente molteplici responsabili[127]. I flussi digitali, infatti, grazie alla persistenza che connota la dimensione temporale dell'informazione, rimangono replicabili all'infinito, offrendo numerose occasioni per comportamenti criminosi: possono essere reindirizzati o inoltrati illegalmente a determinati o indeterminati destinatari, mentre i riceventi hanno la possibilità di eluderli così come di accedervi[128].

Questo aspetto si inserisce all'interno di uno dei rischi che connotano in generale il *Cyberspace,* per come individuati da Bert-Jaap Koops[129]: Internet, secondo l'autore, può infatti "far esplodere" la portata di un crimine, tramutandolo da piccolo inconveniente a grave danno[130]. Quando si tratta, in particolare, di comportamenti criminali sostanziatesi in comunicazioni veicolanti contenuti lesivi di diritti altrui – non solo di carattere diffamatorio, ma pensiamo

[119] Per riferimenti dottrinali cfr. nota n. 108.
[120] Su tale ultima categoria si rimanda a Prosdocimi (1979), pp. 522-553; Prosdocimi (1982).
[121] Cass. Pen., Sez. V, 27 dicembre 2016, n. 54946, in *Foro it.*, 2017, con nota di Di Ciommo (2017), pp. 252-263; e da ultimo, la discussa Cass. Pen., sez. V, 20 marzo 2019, n. 12546, in *Diritto di Internet,* con nota di Guercia (2019), pp. 576-584.
[122] Picotti (2019), p. 90-96, secondo il quale si può parlare di un «evento cibernetico» capace di includere in sé la fase di prolungamento ed estensione del reato che si consuma nel *Cyberspace*. Sul concetto del "prolungamento" degli elementi essenziali del fatto tipico si segnala anche Brunelli (2000), pp. 28-33.
[123] Cass. Pen., Sez. V, 11 dicembre 2017, n. 13398, in *Foro it.,* 2018, 5, 2, cc. 305-309.
[124] Ibidem.
[125] Cass. pen., sez. V, 11 dicembre 2017, n. 13398, in *Foro it.,* 2018, 5, 2, c. 305 ss.
[126] Ansuàtegui Roig (2017), p. 38.
[127] Ibidem.
[128] Khanna (2016), p. 453, così come riportato da Maestri (2017), p. 16.
[129] Koops (2010), p. 735.
[130] Ibidem. Sottolinea l'autore come una fotografia a contenuto sessuale postata *online* acquisisca una portata globale e permanente o come molestie scritte nel cyberspazio integranti ipotesi di bullismo abbiano un impatto molto maggiore di qualsiasi attacco compiuto a scuola. In questo senso anche: Franks (2010), p. 1-10, la quale sottolinea come la fondamentale differenza che connota il *cyber harassment* non sta nei contenuti ma nelle forme: esso non è infatti limitato nel tempo, dal momento che post, commenti, immagini e video integranti molestie sono spesso impossibili da cancellare, impedendo alla vittima di poter superare e dimenticare l'offesa subita.

anche a tutti i casi di *cyber harassment* o di contenuti a sfondo sessuale diffusi senza il consenso del soggetto raffigurato – occorre tenere in considerazione come «il *Cyberspace* faciliti l'amplificazione, l'accrescimento e la permanenza del danno»[131].

In questa prospettiva, la libera disponibilità di un contenuto illecito nel *web* non costituisce un semplice «fattore di aggravamento delle conseguenze del reato»[132], ma comporta invece una *protrazione* dell'offesa al bene giuridico protetto, la quale può così risultare aggravata e approfondita.

Quale conseguenza di tale assunto, la valutazione del fatto tipico va effettuata con riferimento sia al momento del caricamento del dato *online*, sia al momento successivo della permanenza dello stesso in rete, «allo scopo di accertare se, in relazione ad entrambi i momenti, sia in concreto rimproverabile all'imputato la mancata osservanza di regole di condotta, che, ove rispettate, avrebbero impedito la lesione del bene giuridico protetto dalle norme penali»[133].

Questo rilievo ha condotto la dottrina ad interrogarsi sull'esigenza di delineare categorie dogmatiche nuove, capaci di definire e coordinarsi con la pur tradizionale distinzione tra momento di perfezione formale, che in rete si realizza con la prima messa a disposizione del dato, e momento di consumazione sostanziale, che coincide con l'esaurimento del reato, del suo contenuto di offesa, dovuto ad intervento dell'uomo od a ragioni tecniche[134]. Un tale inquadramento dogmatico condurrebbe a rilevanti conseguenze in tema di responsabilità dell'I-SP a titolo di concorso omissivo nel reato commissivo dell'utente. La condotta di mancata consapevole rimozione del contenuto illecito da parte degli ISP non sarebbe più infatti un comportamento qualificabile come *post factum*, ma diventerebbe penalmente rilevante e base per una responsabilità concorsuale per omesso impedimento, rispondendo alle esigenze politico-criminali, che chiedono una maggiore responsabilizzazione anche penale degli operatori in Internet.

Da tutto quanto sopra emerge, in ogni caso, la necessità di una rimodulazione di talune categorie del diritto penale, le quali continueranno a reggersi sui propri tratti costitutivi tipici, ma dovranno essere pervase da un apporto interdisciplinare, che renda possibile regolare e interpretare correttamente in ambito giuridico penale le dinamiche innescate dalle nuove tecnologie[135].

5. I nuovi scenari aperti dal digitale.

Le peculiarità della natura e del funzionamento della realtà digitale hanno ormai permeato molti aspetti dell'esperienza soggettiva. Il particolare funzionamento delle TIC, che va sempre considerato nelle sue componenti tecniche, non si limita infatti a migliorare i risultati delle prestazioni poste in essere per loro tramite, ma «crea e ri-costruisce interamente la realtà che l'utente è in grado di abitare»[136].

E il risultato dell'azione del digitale che percepiamo, in termini di pervasività, non è altro che il risultato del funzionamento del complesso apparato di procedure tecniche che governando la rete, le cui dinamiche necessitano di inserirsi in forme di regolamentazione che possano dare maggior certezza e garanzia di tutela dei diritti fondamentali degli individui.

La natura della vita nel *web* influenza quindi anche i modelli di responsabilità configurabili in capo ai protagonisti della rete, gli *Internet provider*. La scelta, sempre più confermata dalle numerose pronunce giurisprudenziali, nonché dalle recenti evoluzioni in ambito europeo, di concentrare la costruzione di eventuali ipotesi di responsabilità degli intermediari sulla base delle condotte realizzate nel periodo di persistenza dei dati illeciti in rete si articola proprio a partire dalle specifiche dinamiche tecniche che governano il *Cyberspace*. La particolare natura tecnico-informatica del digitale è portatrice infatti di nuove dimensioni, come quella a cui

[131] Franks (2010), p. 3.
[132] Qualifica in questo senso la persistenza dell'informazione lesiva in rete il Tribunale di Torino, nell'ordinanza del 18 dicembre 2018, così come riportata da Cass. pen., sez. V, 13 maggio 2019, n. 20545, inedita.
[133] Ibidem.
[134] Picotti (2019), p. 90-96.
[135] Sabella (2017), p. 143.
[136] Floridi (2017), p. 78. Questa «migrazione» che caratterizza la nostra epoca è diretta, secondo il filosofo dell'informazione, verso quella che egli definisce come l'«infosfera», realtà informazionale fondata sulla contaminazione tra mondo analogico offline e mondo virtuale online, resa possibile dalla grande potenza che connota l'azione delle TIC. Esse, in quanto capaci di condizionare profondamente gli schemi informazionali che costituiscono l'individuo (noi siamo le nostre informazioni), si caratterizzano infatti per essere potenti tecnologie del sé.

conduce la particolare temporalità delle informazioni, che non possono che avere ricadute sui modelli di responsabilità dei soggetti che ne attivano e gestiscono – in diversi modi e parti – il funzionamento.

Partendo da questa consapevolezza e scendendo nel merito della questione che qui si è cercato di ricostruire, è da sottolineare come l'analisi dell'eventuale configurabilità di un regime di responsabilità penale *ex post* degli ISP debba articolarsi su due linee di indagine, diverse ma in necessario rapporto dialettico l'una con l'altra.

La prima riguarda le peculiarità che caratterizzano i reati cibernetici. Quando i comportamenti posti in essere nel *Cyberspace* integrano ipotesi di reato, occorrerà considerare ed esaminare il ruolo e la rilevanza che le componenti tecnico-informatiche, sempre più connotate da un elevato grado di automazione e autonomia – grazie all'impiego delle complesse metodologie del *machine learning* –, assumono nella configurazione della fattispecie criminosa. Diverse voci della dottrina e della giurisprudenza[137] hanno evidenziato come il fatto tipico costitutivo del reato cibernetico debba necessariamente includere anche le fasi di natura tecnica, sostanziate nei diversi processi di codificazione, decodificazione, trattamento, trasmissione e memorizzazione di dati.

Il grado d'automazione dei processi che elaborano sempre più imponenti quantitativi di dati pone importanti dubbi al penalista, primo fra tutti quello concernente le forme di responsabilità prospettabili nei casi di illeciti realizzati attraverso l'impiego di strumenti automatizzati ed autonomi come quelli regolati da algoritmi, sempre più sofisticati e complessi[138]. Il diritto penale infatti, nei casi e modi opportuni e sempre secondo una logica di *extrema ratio*, non può che essere coinvolto nelle logiche di regolamentazione dei comportamenti realizzati nel *Cyberspace*, soprattutto quando tali comportamenti criminosi vanno ad offendere diritti fondamentali e beni giuridici di primaria importanza, a partire dall'integrità dello sviluppo psico-fisico dei minori.

La seconda linea d'indagine riguarda invece la valorizzazione della previsione di precisi obblighi di notifica e rimozione, ai quali gli intermediari dovranno conformarsi; obblighi diversificati sulla base di diversi parametri – tra i quali, il più rilevante sarà il grado di illiceità del contenuto disponibile in rete così come la sua portata offensiva – aventi ad oggetto l'adozione di misure tecnico-organizzative volte alla individuazione e rimozione di contenuti illeciti in rete. È grazie alla formalizzazione di queste procedure che si avranno gli elementi necessari per l'eventuale costruzione di una responsabilità penale dell'intermediario per concorso omissivo nel reato realizzato dai propri utenti.

La previsione di un simile regime darebbe certezza ai prestatori, i quali avrebbero in mano un efficace strumento per andare esenti da responsabilità, dimostrando di essersi conformati agli obblighi attraverso l'adozione delle misure necessarie.

Un sistema di questo tipo sarebbe, peraltro, facilmente compatibile con la natura degli intermediari, per la maggior parte soggetti privati, che agiscono quali aziende complesse e, quindi, attraverso strutture e logiche organizzative d'impresa[139]. In questo modo si costruirebbero forme di responsabilità basate non solo sulla natura illecita del contenuto ospitato, quanto piuttosto su di una «responsabilità organizzativa»[140] («*responsibility for the design of organizations*»[141]), derivante dall'aver disegnato la piattaforma in modo da non essere in grado di controllare, prevenire o rimuovere la disponibilità di contenuti illeciti accessibili o gestiti dagli utenti[142].

Tale soluzione sembra essere, peraltro, in linea con le posizioni evincibili dalle diverse fonti europee in materia, sia giurisprudenziali che normative, le quali, per quanto siano ancora in una fase di definizione ed assestamento, quando affrontano la complessa tematica della regolamentazione di ciò accade nel *Cyberspace*, convengono nel ritenere necessario e imprescindibile il coinvolgimento degli *Internet provider*.

Questi soggetti rivestono infatti un ruolo sempre più rilevante nella gestione di servizi e

[137] Picotti (2019), p. 35 ss. Cfr. nello stesso senso Picotti (2011), p. 843; Pica (2004), p. 425; Catullo (2003), p. 3963; Cornils (2002), p. 891. In giurisprudenza: Sezioni Unite della Corte di Cassazione in materia di accesso abusivo, sentenza del 24 aprile 2015, n. 17325, in *Dir. pen. e proc.*, 2015, n. 10, p. 1291 ss., con nota di Flor, cfr. in particolare p. 1299.
[138] Sul tema si segnalano: Kroll *et al.* (2016), pp. 1-66; Fioriglio (2015), pp. 113-141; Pagallo (2013).
[139] La scelta di imporre alle imprese l'adozione di opportune misure tecnico-organizzative quale soluzione alle diverse minacce *cyber* richiama, peraltro, il regime di *accountability* delineato dal GDPR, punto che meriterebbe ulteriori approfondimenti.
[140] Montagnani (2018), p. 200, concetto che si sposa con quello di *cooperative responsibility* sopra menzionato (cfr. Helberger *et al.* (2018), pp. 1-14). Nello stesso senso anche montagnani e Trapova (2018), p. 296.
[141] Helberger *et al.* (2018), p. 4.
[142] Montagnani (2018), p. 200.

piattaforme, arrivando ad influenzare la nostra quotidianità, che si articola ormai in gran misura tramite quelle stesse piattaforme. La circostanza per cui circa 30 *corporations* controllano il 90% del traffico mondiale della rete[143], e che procedure d'analisi e rimozione di contenuti illeciti sono diventate "una questione privata", mostrano come il continuare a qualificare gli intermediari quali meri «operatori tecnici e neutrali»[144] sia una via ormai da abbandonare.

Bibliografia

Abbondante, Fulvia (2017): "Il ruolo dei social network nella lotta all'*hate speech*: un'analisi comparata fra l'esperienza statunitense e quella europea", *Informatica e diritto*, 1-2, pp. 41-68

Allegri, Maria Romana (2017): "Alcune considerazioni sulla responsabilità degli intermediari digitali, e particolarmente dei *social network provider*, per i contenuti prodotti dagli utenti", *Informatica e diritto*, 1-2, pp. 69-112

Amato Mangiameli, Agata (2017): "Tecno-regolazione e diritto. Brevi note su limiti e differenze", *Diritto dell'Informazione e dell'Informatica*, pp. 147-167

Ansuàtegui Roig Francisco Javier (2017): "Libertà di espressione, discorsi d'odio, soggetti vulnerabili: paradigmi e nuove frontiere", *Ars interpretandi,* 1, pp. 29-48

Bartoli, Roberto (2013): "Brevi considerazioni sulla responsabilità penale dell'*Internet Service Provider*", *Diritto penale e processo*, 5, pp. 600-606

Berlingò, Vittoria (2017): "Il fenomeno della *datafication* e la sua giuridicizzazione", *Rivista trimestrale di diritto pubblico*, 4, pp. 641- 675

Bisori, Luca (1997): "L'omesso impedimento del reato altrui nella dottrina e giurisprudenza italiane", Rivista italiana di diritto e procedura penale, pp. 1339-1394

Bocchini, Roberto (2017): "Responsabilità dell'*hosting provider* – la responsabilità di Facebook per la mancata rimozione dei contenuti illeciti", *Giurisprudenza italiana*, pp. 632-643

Brunelli, Daniele (2000): *Il reato portato a conseguenze ulteriori. Problemi di qualificazione giuridica* (Torino, Giappichelli)

Bugiolacchi, Leonardo (2013): "Evoluzione dei servizi di *hosting provider*, conseguenze sul regime di responsabilità e limiti dell'attuale approccio *case by case*", *Responsabilità civile e previdenza*, pp. 1997-2007

Caletti Gian Marco (2018): "*Revenge porn* e tutela penale", *Diritto penale contemporaneo Rivista trimestrale,* 3, pp. 63-100

Cassano, Giuseppe (2017): Stalking*, atti persecutori, cyberbullismo e diritto all'oblio* (Milano, Wolters Kluwer)

Catullo Francesco Giuseppe (2019): "La responsabilità penale del direttore del giornale telematico tra legislatore pigro e giudice intraprendente", *Diritto di Internet,* 1, pp. 173-177

Catullo Francesco Giuseppe, *Diffamazione telematica attraverso la decontestualizzazione dell'identità,* in *Cass. pen*., 2003, pp. 3963-3970.

[143] Maestri, Lex inforamtica *e diritto,* cit., p. 15.
[144] Sul superamento della teoria della neutralità cfr. Allegri, Ubi Social, Ibi Ius, cit., p. 224 s.; Thompson, *Beyond Gatekeeping,* cit., p. 785 ss. il quale si chiede, visto il grande potere che hanno gli intermediari, "censori ufficiosi" della rete che decidono cosa è legale e cosa non lo è: «non è forse peggio per la libertà di espressione, e in definitiva per la legge stessa, se le loro decisioni non vengono controllate? (…) Le risorse e la saggezza che gli intermediari investono nel raggiungere tali decisioni saranno, infatti, tanto potenti quanto gli intermediari stessi. Peggiore sarà l'intermediario, peggiore sarà la decisione; più è potente l'intermediario, più pervasivo sarà l'effetto di quella stessa decisione».

Codiglione, Giorgio Giannone (2017): "La nuova legge tedesca per l'*enforcement* dei diritti sui social media", Diritto dell'Informazione e dell'Informatica, pp. 723-735

Colangelo, Giuseppe (2017): "*Digital Single Market Strategy*, diritto d'autore e responsabilità delle piattaforme *online*", *Analisi Giuridica dell'Economia*, 2, pp. 603-637

Colangelo, Giuseppe e Maggiolino, Mariateresa (2018): "ISP's copyright liability in the EU digital single market strategy", *Informational Journal of Law and Information Technology*, 26, pp. 142-159

Colangelo, Giuseppe e Torti, Valerio (2019): "Copyright, online news publishing and aggregators: a law and economic analysis of the EU reform", *International Journal of Law and Information Technology*, 27, pp. 75-90

Cornils Karin, *Il luogo di commissione dei reati di manifestazione del pensiero in Internet*, in *Diritto dell'Informazione e dell'Informatica,* 2002, n. 4-5, pp. 891-901.

Curreli Carlo (2017): "La diffamazione su facebook, tra diritto sostanziale e profili probatori", *Responsabilità civile e previdenza,* 1, pp. 189-198.

D'Ambrosio, Luca (2012): "Responsabilità degli *Internet provider* e Corte di Giustizia dell'Unione Europea: quali spunti per il sistema penale italiano?" in Luparia, Luca (eds.): Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale* (Milano, Giuffrè), pp. 67-93

D'Ippolito, Guido (2017): "L'esigenza di un nuovo bilanciamento per il diritto d'autore: gli *user generated content* e l'ipotesi di un'eccezione per le opere creative e trasformative", *Cyberspazio e Diritto*, 3, pp. 513-569

De Cata, Marcello (2010): *La responsabilità civile dell'*internet provider (Milano, Giuffrè)

Delsignore Stefano (2019): "La tutela dei minori e la pedopornografia telematica: i rati dell'art. 600 ter c.p"., in Cadoppi Alberto, Canestrari Stefano, Manna Adelmo, Papa Michele (eds.): *Cybercrime*, (Milano, Utet Giuridica), pp. 374-486

Di Ciommo, Francesco (2010): "Programmi filtro e criteri di imputazione/esonero della responsabilità *online*. A proposito della sentenza Google/ViviDown", *Diritto dell'Informazione e dell'Informatica*, pp. 829-857

Di Ciommo, Francesco (2017): "Responsabilità dell'*Internet hosting provider*, diffamazione a mezzo Facebook e principio di tassatività della norma penale: troppa polvere sotto il tappeto", *Foro Italiano,* pp. 252-263

Di Tano, Francesco (2017): "Prospettive *de jure condendo* sulla responsabilizzazione dei *content provider*", *Informatica e diritto*, 1-2, pp. 113-126

Falconi, Federica (2016): "La responsabilità dell'*Internet service provider* tra libertà di espressione e tutela della reputazione altrui", *La Comunità Internazionale*, 71, 2, pp. 235-254

Fiandaca, Giovanni (1979): *Il reato commissivo mediante omissione* (Milano, Giuffrè)

Fiandaca, Giovanni (1983): "Reati omissivi e responsabilità penale per omissione", *Foro Italiano*, 106, V, cc. 27-45

Fiandaca, Giovanni (2005): "Il giudice di fronte alle controversie tecnico-scientifiche. Il diritto e il processo penale", *Diritto & questioni pubbliche*, 5, pp. 1-23

Finocchiaro, Giusella e Avitabile, Alberto (2017): *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali* (Torino, Giappichelli)

Fioriglio, Gianluigi (2015): "La "dittatura" dell'algoritmo: motori di ricerca web e neutralità della indicizzazione. Profili informatico-giuridici", *Bocconi Legal Papers*, 3, pp. 113-141

Flor Roberto (2015): "I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite", in *Diritto penale e processo,* n. 10, pp. 1296-1309

Flor Roberto (2017): "Cyber-terrorismo e diritto penale in Italia", in Wenin R, Fornasari G. (eds.): *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali,* (Trento, Quaderni Facoltà di Giurisprudenza), pp. 325-362

Flor, Roberto (2010): *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet. Un'indagine comparata in prospettiva europea ed internazionale* (Padova, Cedam)

Flor, Roberto (2012): "*Social network* e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità del fornitore del servizio?", *Rivista trimestrale di diritto penale dell'economia,* 3, pp. 647-693

Floridi, Luciano (2015): "Introduction", in Floridi, Luciano (eds.): *The Onlife Manifesto. Being Human in a Hyperconnected Era,* disponibile sul sito https://www.springer.com

Floridi, Luciano (2017): *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo* (Milano, Raffaello Cortina)

Franks Mary Anne (2010): "The banality of cyber discrimination, or, the eternal recurrence of September", *Denver Law Review Online,* 87, pp. 1-6

Frosio Giancarlo (2018): "Why keep a dog and bark yourself? From intermediary liability to responsibility", *International Journal of Law and Information Technology*, 26, pp. 1-33

Grasso, Giovanni (1983): *Il reato omissivo improprio* (Milano, Giuffrè)

Helberger Natali *et al.* (2018): "Governing online platforms: From contested to cooperative responsibility", *The Information Society*, 34:1, pp. 1-14

Ingrassia, Alex (2012): "Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine? Le responsabilità penali dei *provider* nell'ordinamento italiano", in Luparia, Luca (eds): *Internet* provider *e giustizia penale*, (Milano, Giuffrè)

Khanna Parag (2016): *Connectography: Mapping the Future of Global Civilization*, (Penguin Press, New York)

Koops Bert-Jaap (2010): "The internet and its opportunities for cybercrime", in M. Herzog-Evans (eds.): *Transnational Criminology Manual,* (Wolf Legal Publishers, Nijmegen), pp. 1-12

Kroll, Joshua *et al.* (2016): "Accountable Algorithms", *University of Pennsylvania Law review*, 165, pp. 1-66

Leoncini, Isabella (1999): *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza* (Torino, Giappichelli)

Lessing, Lawrence (2006): *Code 2.0*, disponibile al sito http://codev2.cc/download+remix/Lessig-Codev2.pdf.

Luberto, Mario e Zanetti, Gian Francesco (2008): "Il diritto penale dell'era digitale. Caratteri, concetti e metafore", *Indice penale*, pp. 497-510

Maestri Enrico (2017): "Lex inforamtica *e diritto. Pratiche sociali, sovranità e fonti nel* cyberspazio", *Ars interpretandi,* 1, pp. 15-28

Manna, Adelmo (2001): "Considerazioni sulla responsabilità penale dell'*Internet provider* in tema di pedofilia", *Diritto dell'Informazione e dell'Informatica*, pp. 145-151

Manna, Adelmo e Di Florio Mattia (2019): "Riservatezza e diritto alla privacy: in particolare, la responsabilità per omissione dell'*internet provider*", in Cadoppi, Alberto *et al.* (eds.): *Cybercrime* (Milano, Utet Giuridica), pp. 891-940

Mauri Roberta Eleonora (2019): "Applicabile l'art. 57 c.p. al direttore del quotidiano online: un revirement giurisprudenziale della Cassazione, di problematica compatibilità con il divieto di analogia", *Diritto penale contemporaneo,* disponibile al sito https://www.penalecontemporaneo.it/d/6501-applicabile-lart-57-cp-al-direttore-del-quotidiano-online-un-revirement-giurisprudenziale-della-cas

Mcluhan, Marshall (1967): *Gli strumenti del comunicare* (Milano, Il Saggiatore)

Militello, Vincenza (2014): "L'identità della scienza giuridica penale nell'ordinamento multilivello", *Rivista italiana di diritto e procedura penale*, pp. 106-132

Montagnani, Maria Lillà (2018): *Internet, contenuti illeciti e responsabilità degli intermediari*, (Milano, Egea)

montagnani, Maria Lillà e Trapova, Alina (2018): "Safe harbours in deep waters: a new emerging liability regime for Internet intermediaries in the Digital Single Market", *International Journal of Law and Information Technology*, 26, pp. 294-310

Montanari, Matteo (2017): "La responsabilità delle piattaforme *online* (il caso Rosanna Cantone)", *Diritto dell'Informazione e dell'Informatica*, pp. 254-283

Nordemann, Jan Bernd (2017): "Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?", disponibile al sito http://www.europarl.europa.eu.

Pagallo, Ugo (2013): *The Laws of Robots: Crimes, Contracts, and Torts* (Berlino, Springer)

Pascuzzi, Giovanni (2016): *Il diritto dell'era digitale* (Bologna, Il Mulino)

Petrini Davide (2017): "Diffamazione online: offesa recata con "altro mezzo di pubblicità?" o col mezzo della stampa?", *Diritto penale e processo,* 11, pp. 1485-1492

Petrini, Daniele (2004): *La responsabilità penale per i reati via internet* (Napoli, Jovene)

Petruso, Rosario (2018): "Responsabilità delle piattaforme *online*, oscuramento di siti web e libertà di espressione nella giurisprudenza della Corte europea dei diritti dell'uomo", *Diritto dell'Informazione e dell'Informatica*, pp. 511-558

Pica Giorgio (2004): "Internet (diritto penale)", voce in *Digesto delle discipline penalistiche*, *Aggiornamento* (Utet, Milano), pp. 425-483

Picotti Lorenzo (2006): "Sub art. 600 ter III comma c.p.", in Cadoppi Alberto (eds.): *Commentario delle norme contro la violenza sessuale e contro la pedofilia,* IV ed., (Padova, Cedam), pp. 175-212

Picotti, Lorenzo (1999): "La responsabilità penale dei *service providers* in Italia", *Diritto penale e processo*, 4, pp. 501-506

Picotti, Lorenzo (2004): "Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati," in Picotti, Lorenzo (eds.): *Il diritto penale dell'informatica nell'epoca di Internet* (Padova, Cedam)

Picotti, Lorenzo (2007): "La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in Internet (L. 6 febbraio 2006, n. 38) (Parte seconda)", *Studium Iuris*, 11, pp. 1196-1211

Picotti, Lorenzo (2011): "La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee", *Rivista trimestrale di diritto penale dell'economia*, 4, pp. 827-864

Picotti, Lorenzo (2012): "I diritti fondamentali nell'uso ed abuso dei *social network*. Aspetti penali", *Giurisprudenza di merito*, pp. 2522-2547

Picotti, Lorenzo (2019): "Diritto penale e tecnologie informatiche: una visione d'insieme", in Cadoppi, Alberto *et al.* (eds.): *Cybercrime* (Milano, Utet Giuridica), pp. 33-96

Piraino, Fabrizio (2017): "Spunti per una rilettura della disciplina giuridica degli *internet service provider*", *Annali italiani del diritto d'autore*, 1, pp. 152-200

Pollicino Oreste (2014): "Internet nella giurisprudenza delle Corti europee: prove di dialogo?", *Diritto dell' Unione eu*ropea, 3, pp. 601 ss.

Pollicino, Oreste (2014): "Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli *Internet service provider*", disponibile al sito: http://www.giurcost.org

Prosdocimi, Salvatore (1979): "Osservazioni sull'aggravamento o tentato aggravamento delle conseguenze del delitto commesso", *Rivista italiana di diritto e procedura penale*, pp. 522-553

Prosdocimi, Salvatore (1982), *Profili penali del postfatto*, (Milano, Giuffrè)

Romano, Mario (1995): *Commentario sistematico del codice penale*, *sub. Art. 40* (Milano, Giuffrè), pp. 337-366

Ruggiero, Francesco (2001): "Individuazione nel ciberspazio del soggetto penalmente responsabile e ruolo dell'*internet provider*", *Giurisprudenza di merito*, pp. 586-602

Sabella, Pietro (2017): "Il fenomeno del *cybercrime* nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di Internet per fini di terrorismo, tra esigenze di sicurezza e rispetto dei diritti fondamentali", *Informatica e diritto*, 26, 1-2, pp. 139-176

Salvadori, Ivan (2007): "I presupposti della responsabilità penale del *blogger* per gli scritti offensivi pubblicati su un blog da lui gestito", *Giurisprudenza di merito,* pp. 1069-1079

Salvadori, Ivan (2011): "La normativa penale della stampa non è applicabile, *de jure condito*, ai giornali telematici", *Cassazione penale,* pp. 2982-2994

Sammarco Pieremilio (2012): "Alla ricerca del giusto equilibrio da parte della Corte di Giustizia UE nel confronto tra diritti fondamentali nei casi di impiego di sistemi tecnici di filtraggio", *Diritto dell'Informazione e dell'Informatica,* 2, pp. 297-305

Scardino, Francesco (2015): "Una analisi del "Decreto antiterrorismo" Commento a d.l. 18 febbraio 2015, n. 7", *Rassegna Avvocatura dello Stato*, 2, pp. 215-239

Scialdone, Mario (2013): "Il nuovo ruolo degli utenti nella generazione di contenuti creativi", *Diritto Mercato Tecnologia*, 4, pp. 8-19

Seminara, Sergio (1997): "La pirateria su Internet e il diritto penale", *Rivista trimestrale di diritto penale dell'economia*, 3, pp. 71-114

Seminara, Sergio (1998): "La responsabilità penale degli operatori su internet", *Diritto dell'Informazione e dell'Informatica*, pp. 745-774

Seminara, Sergio (2014): "Internet (diritto penale)", *Enciclopedia del Diritto, Annali VII* (Milano, Giuffrè), pp. 567-606

Sgubbi, Filippo (1975): *Responsabilità penale per omesso impedimento dell'evento* (Padova, Cedam)

Shapiro, Andrew (2000): *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know* (New York, PublicAffairs)

Sieber, Ulrich (1997), "Responsabilità penali per la circolazione di dati nelle reti internazionali di computer. Le nuove sfide di Internet (II parte)", *Rivista trimestrale di diritto penale dell'economia*, 4, pp. 1193-1232

Smythe, Dallas (2009): "On the Audience Commodity and Its Work", in Durham, Meenakshi Gigi e Kellner, Douglas (eds.): *Media and Cultural Studies* (Malden, Blackweel), pp. 230-256

Spagnoletti, Valeria (2004): "La responsabilità del *provider* per i contenuti illeciti di Internet", *Giurisprudenza di merito*, 9, pp. 1922-1937

Tabarelli de Fatis Stefania (2013): "Prospettive di riforma del delitto di diffamazione, con particolare riferimento alla diffamazione *online*", in Picotti Lorenzo (eds.): *Tutela penale della persona e nuove tecnologie,* (Padova, Cedam), pp. 193-239

Torre, Valeria (2013): "Sulla responsabilità penale del *service provider* e la definizione del comportamento esigibile alla luce delle norme contro la pedopornografia", in Picotti, Lorenzo (eds.): *Tutela penale della persona e nuove tecnologie*, (Padova, Cedam), pp. 163-191

Tosi, Emilio (2017): "Contrasti giurisprudenziali in materia di responsabilità civile degli *hosting provider* – passivi e attivi – tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti", *Rivista di Diritto Industriale*, 1, pp. 75-122

Van Vegchel, Jan (2018): "European Council's amended proposal for a Directive on copyright in the Digital Single Market; is it enough to ward off threat to press freedom?", *SSRN Electronic Journal*, pp. 1-9

Vigliar, Salvatore (2018): "Pirate Bay: evoluzione del concetto di comunicazione al pubblico o nuova frontiera della responsabilità delle piattaforme telematiche?", *Diritto dell'Informazione e dell'Informatica*, pp. 108-122

Diritto penale e libertà di espressione in internet

El derecho penal y la libertad de expresión en internet

Criminal Law and Freedom of Expression on the Internet

Istanze di criminalizzazione delle *fake news* al confine tra tutela penale della verità e repressione del dissenso

La criminalización de las fake news entre al confín entre tutela penal de la verdad y represión del disenso

Criminalisation of Fake News Between the Protection of Truth and the Suppression of Dissent

Anna Costantini
Dottoranda di ricerca in Diritti e Istituzioni – Diritto penale presso l'Università degli Studi di Torino
anna.costantini@unito.it

Libertà di espressione, Diffamazione | Libertad de expresión, Difamación | Freedom of expression, Defamation

Abstracts

Il contributo si propone di esaminare nella prospettiva del diritto penale il problema della divulgazione di *fake news* tramite i *social media*, sia al fine di valutare se le condotte di diffusione di false notizie tramite il *web* possano già dar luogo a forme di responsabilità penale, sia al fine di sottoporre a vaglio critico le ragioni di politica criminale sottese alle istanze di espansione della punibilità che trovano espressione in numerose proposte legislative. Tali istanze devono essere valutate alla luce della più ampia tematica dell'impiego dello strumento punitivo in chiave di tutela della verità delle informazioni trasmesse al pubblico, cui si correla la questione dei limiti costituzionali all'incriminazione di condotte che si estrinsecano nella manifestazione di un pensiero, come tali astrattamente rientranti sotto la copertura dell'art. 21 Cost. In definitiva, si tratta di capire se le nuove istanze di criminalizzazione delle *fake news* rispondono a effettive esigenze di tutela ovvero si risolvono in una mera strumentalizzazione delle valenze simboliche del diritto penale in chiave di repressione delle opinioni di dissenso.

El presente trabajo tiene por objeto examinar desde la perspectiva del derecho penal el problema de la divulgación de fake news a través de redes sociales. Junto con analizar si las conductas de difusión de noticias falsas a través de internet pueden ya dar lugar a formas de responsabilidad penal, se revisa críticamente las razones de política criminal subyacentes a varias propuestas legislativas que buscan expandir la punibilidad en estos casos. Tales propuestas deben evaluarse a la luz de una temática más amplia: el de la utilización de la herramienta penal para tutelar la verdad de las informaciones trasmitidas al público, lo cual plantea la cuestión de los límites constitucionales a la incriminación de conductas que constituyen la manifestación o expresión de un pensamiento. En definitiva, se trata de resolver si las nuevas instancias de criminalización de las fake news responden a efectivas exigencias de tutela penal o si, en cambio, constituyen una mera instrumentalización simbólica del derecho penal en clave de represión de las opiniones de disenso.

The paper focuses, from a criminal law perspective, on the dissemination of fake news through social media, in order to assess if it can amount to a crime and to scrutinize the criminal policy reasons behind several bill drafts proposing to punish such behavior. The said reasons must be assessed in light of the protection of truth with respect to the information to the general public, including the constitutional limits related to the criminalization of free expression (under article 21 of the Italian Constitution). After all, the point is understanding to what extent criminalizing fake news is consistent with the criminal policy as a whole, or they are rather a way to use criminal law as a tool for the suppression of dissent.

Sommario

1. *Fake news*, ossia la falsità delle notizie all'epoca di internet e della post-verità.

Tra le manifestazioni più recenti della tendenza espansiva del diritto penale, un tema delicato è quello relativo alla richiesta, proveniente da una parte dell'opinione pubblica, di interventi punitivi vòlti a contrastare la diffusione tramite *internet* di notizie false, fenomeno che, negli ultimi anni, ha assunto dimensioni particolarmente estese e alimentato una percezione sociale di crescente pericolo. Di fronte alle istanze di allargamento dell'area del penalmente rilevante, rese concrete dalla presentazione di numerosi progetti di legge in Parlamento, il compito che si richiede allo studioso di diritto penale è quello di verificare la sussistenza o meno di reali lacune di tutela, tali da evidenziare l'inadeguatezza dell'attuale compendio sanzionatorio e da non poter essere colmate neppure mediante il ricorso a rimedi di carattere extra-penale. La riflessione sul rapporto tra diritto penale e *fake news* – così sono ormai comunemente indicate le false notizie circolanti *online* – si innesta, poi, nella più ampia tematica dell'impiego dello strumento punitivo in chiave di tutela della *verità* delle informazioni trasmesse al pubblico, cui si correla la questione dei *limiti costituzionali* all'incriminazione di condotte che si estrinsecano nella manifestazione di un pensiero, come tali astrattamente rientranti sotto la copertura dell'art. 21 Cost..

Nel tentativo di offrire un contributo di riflessione in tal senso, occorre muovere da un inquadramento generale del fenomeno di cui si parla. Quel che colpisce, a un approccio iniziale, è l'apparente *novità* del problema: se di "false notizie" è costellata l'intera storia dell'umanità[1], di "*fake news*" si è iniziato a parlare solo da un paio d'anni, precisamente da quando l'espressione fu impiegata dai *mass media* americani – e, subito, importata da quelli italiani – per indicare l'incidenza delle "bufale" diffuse tramite *social networks* per favorire la vittoria di Donald Trump alle elezioni presidenziali americane del 2016[2].

Da allora, l'anglicismo ricorre continuamente nel linguaggio giornalistico e politico, a evidenziare come la propagazione di notizie false assuma dimensioni e connotati affatto peculiari in connessione con lo sviluppo di internet e dei *social media*. Invero, l'assunto che pare dominare la discussione intorno alle *fake news* è quello secondo cui la trasmissione di informazioni non veritiere esprimerebbe una *maggiore pericolosità* laddove sia realizzata attraverso la rete, anziché mediante i tradizionali canali di comunicazione.

Sul piano contenutistico, le *fake news* non si differenziano dai tradizionali meccanismi disinformativi, indicando le notizie che trasmettono al lettore un'erronea corrispondenza tra i fatti narrati e la realtà ("*appearing to be something it is not*"[3]), e possono consistere sia in testi sia in immagini[4]: oltre che i falsi *tout court*, vi rientrano anche le informazioni che, pur possedendo un contenuto di verità, sono manipolate o esposte in modo tendenzioso o fazioso, tali da risultare ingannevoli e fuorvianti. Come si è anticipato, dunque, quel che segna la specificità delle

[1] La diffusione di notizie false quale mezzo usato dal potere per consolidarsi costituisce una costante che attraversa tutte le epoche storiche: uno dei primi esempi riscontrati è la falsa vittoria celebrata dal faraone Ramset II nella battaglia di Qadesh contro gli ittiti, risalente al 1275 a.C.; più celebre è il falso medievale della *Donazione di Costantino*, creato per giustificare il potere temporale della Chiesa e smascherato dall'umanista Lorenzo Valla nel 1440; come pure sono noti i *Protocolli dei Savi di Sion* elaborati dalla polizia zarista nella Russia dei primi del Novecento al fine di fomentare la propaganda antisemita.

[2] Ferraresi, "Genesi delle fake news", in *IlFoglio* (online), 19 febbraio 2019.

[3] Zanon (2018), p. 2. Secondo la definizione, più ristretta, di Allcott e Gentzkow (2017), p. 211, le *fake news* indicherebbero le notizie intenzionalmente false, idonee a ingannare il destinatario e/o non suscettibili di essere verificate.

[4] La manipolazione di immagini e fotografie non è un fenomeno nuovo. Oggi, attraverso la tecnica informatica c.d. "*deepfake*", basata sulla sovrapposizione di immagini facciali, è possibile anche creare video falsi che sembrano veri o manipolare video veri con particolari falsi: in tal modo, potrebbero essere mostrati accadimenti mai verificatisi, o attribuire a personaggi pubblici frasi mai pronunciate (cfr. Monti, "*Deepfake*, i rischi "politici": per la democrazia e l'informazione online", in *agendadigitale.eu*).

fake news rispetto alle "vecchie" menzogne non è la tipologia di messaggio da esse veicolato, bensì il particolare *mezzo* con cui le stesse raggiungono i destinatari, vale a dire la rete *internet*, che rappresenta uno strumento sempre più diffuso tra la popolazione, non solo giovanile[5].

Più precisamente, il carattere aperto del *web* amplifica la *quantità* e la *velocità di circolazione* delle false notizie, che assumono spesso dimensioni virali grazie al meccanismo delle condivisioni "a cascata" degli utenti dei *social networks*[6]. Con l'ampliamento della platea dei soggetti produttori di informazione, tendenzialmente sottratti al rispetto delle sanzioni e delle regole previste per la stampa cartacea e, per di più, legittimati all'anonimato, diviene meno agevole la verifica da parte dei lettori in ordine alla provenienza e all'attendibilità dei dati[7]. In questa prospettiva, la diffusione di *fake news* sarebbe correlata al processo di "disintermediazione" dell'informazione[8], non più necessariamente veicolata da un gruppo ristretto di operatori qualificati: *internet*, infatti, ha rivoluzionato il tradizionale rapporto tra *mass media* e cittadini, consentendo potenzialmente a chiunque di trasformarsi da passivo destinatario e fruitore di informazioni ad attivo produttore o comunicatore delle stesse[9].

La potenzialità decettiva delle *fake news* è, poi, aggravata da fattori sociali quali incultura, credulità collettiva o, addirittura, analfabetismo funzionale[10], che espongono il pubblico a una attenuata capacità di riconoscere persino le notizie palesemente false[11]. Anche a prescindere da tali aspetti patologici, si è osservato come l'attività di fruizione delle informazioni *online* sia inevitabilmente influenzata dai meccanismi algoritmici di organizzazione e di presentazione dei dati, che consentono di portare all'attenzione immediata di ciascun utente notizie selezionate sulla base delle sue preferenze, sia commerciali sia (quel che più preoccupa) di opinione, a loro volta "calcolate" in relazione alle precedenti ricerche o ai tempi di visualizzazione dei contenuti. Tale fenomeno, in particolare, conduce all'isolamento degli internauti in "bolle di filtraggio" (*filter bubbles*), in cui gli stessi ricevono solo informazioni in linea con i propri interessi e con le proprie opinioni, con un conseguente effetto di rafforzamento dei convincimenti anteriori (c.d. *eco chamber*)[12].

Tutti gli elementi descritti spiegano perché il *web* costituisca, a parere di molti, un terreno fertile per la diffusione di notizie false, contribuendo a creare un contesto di generalizzata disinformazione. Il tema ha acquisito un rilievo tale nel dibattito pubblico da essere descritto come vera e propria cifra culturale e filosofica del tempo storico in cui viviamo: secondo una narrazione diffusa, quella attuale sarebbe divenuta un'epoca di *post-verità*[13], dominata cioè dall'indifferenza per la ricerca della verità oggettiva dei fatti e dall'affidamento delle scelte e delle opinioni individuali a impulsi meramente emozionali. È l'emozione suscitata dalle notizie, e non la razionale ponderazione di esse, ad orientare le decisioni di voto degli individui, esattamente come l'emozione indotta da una pubblicità determina le scelte di acquisto dei consumatori, secondo un processo di pervasione dell'area dell'informazione e delle opinioni politiche da parte di logiche pubblicitarie e di mercato.

Gli effetti negativi del fenomeno si riscontrano in diversi ambiti, cui possono essere correlate distinte tipologie di *fake news* in relazione all'origine e alla finalità[14].

L'aspetto del fenomeno che desta maggiore allarme è la lamentata incidenza delle false notizie *online* sullo stesso funzionamento *democratico* delle società attuali, attraverso l'alterazione

[5] Secondo il XII Rapporto Censis-Ucsi del 2015, a utilizzare internet è il 70,9% della popolazione italiana (il 91,9% dei giovani e il 27,8% degli anziani). Per approfondimenti si veda Monti (2017), p. 83.

[6] In particolare, sul ruolo dei *social networks* nella diffusione di notizie false cfr. ancora Monti (2017), p. 83. Si veda anche Sustein (2014), pp. 97-102.

[7] Pinelli (2017), p. 43. In senso critico rispetto all'eventualità di imporre un divieto di anonimato online, v. Melzi D'Eril (2017), p. 65.

[8] Bassini e Vigevani (2017), p. 15.

[9] Zanon (2018), p. 1.

[10] Secondo i dati Ocse del 2016, il 27,9% degli italiani compresi tra 16 e i 65 anni è analfabeta funzionale, cioè ha difficoltà a comprendere brevi testi o a compiere facili operazioni di calcolo nella vita quotidiana
Càndito, "Il 70 per cento degli italiani è analfabeta (legge, guarda, ascolta ma non capisce)", in *La Stampa* (online), 10 gennaio 2017.

[11] Secondo il *report* "Infosfera", realizzato dal gruppo di ricerca sui mezzi di comunicazione di massa dell'Università Suor Orsola Benicasa di Napoli, l'82% degli italiani non sarebbe in grado di distinguere una bufala che circola sul *web*. Sul rapporto tra informazione e fenomeni cognitivi v. anche Mocanu *et al*, 2015, p. 1198 ss.

[12] Pariser (2012), *passim*; Pitruzzella (2017), pp. 64-69; De Gregorio (2017), p. 94.

[13] "*Post-truth*" è il termine dell'anno 2016 per l'Oxford English Dictionary, che così lo definisce: "*relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief*". Sul tema, nella letteratura filosofico-giuridica, cfr. Fioriglio (2016), pp. 1-19; Savarese (2018), pp. 1-21.

[14] La classificazione che segue riprende, in parte, quella proposta da Melzi d'Eril (2017), pp. 63-64, e da Bassini e Vigevani (2017), pp. 15-16.

dei risultati elettorali e l'inquinamento del dibattito e delle decisioni politiche[15]. In relazione a questo profilo, la creazione di contenuti falsi è, per lo più, attribuibile a gruppi di potere (politici o economici) interessati a controllare l'opinione delle masse e, per il tramite, a indirizzare le politiche governative.

In altri casi, le *fake news* sono finalizzate alla realizzazione di profitti, sfruttando le inserzioni pubblicitarie delle pagine *internet* su cui sono ospitate: il meccanismo si basa sulla creazione di titoli accattivanti o sensazionalistici, che attirano l'attenzione degli utenti dei social network e li inducono a cliccare su *link* che rimandano a siti separati (fenomeno del c.d. *click bait*)[16]. Il fine di profitto è, poi, all'origine della creazione e della diffusione di false notizie capaci di produrre alterazioni del mercato e della Borsa.

Infine, le *fake news* proliferano anche al di fuori di specifici (o, quantomeno, riconoscibili) interessi politici o economici sottostanti, alimentandosi di credenze popolari antiscientifiche (si pensi alle *fake news* correlate alla campagna *no vax*) ovvero di intenzioni offensive individuali (ad esempio, campagne diffamatorie, espressioni razziste o comunque discriminatorie, discorsi incitanti all'odio – c.d. *hate speech*[17] – verso singole persone o gruppi). Rispetto a tali ipotesi, lo strumento informatico ha l'effetto di amplificare la risonanza delle informazioni fallaci, che raggiungono un gruppo particolarmente ampio di destinatari, accentuando i pericoli per i beni collettivi o individuali coinvolti.

L'insieme degli aspetti problematici legati alla proliferazione di *fake news* tramite *web* ha ingenerato preoccupazione nell'opinione pubblica, favorendo il sorgere di correnti di pensiero favorevoli all'introduzione di forme di regolamentazione e controllo della rete, anche mediante l'utilizzo dello strumento penale.

A fronte di tali istanze, si tratta anzitutto di analizzare lo stato attuale della legislazione penale, al fine di verificare se e a quali condizioni la diffusione di contenuti falsi *online* possa già assumere rilevanza penale. Successivamente, sarà necessario prendere in esame le principali proposte normative – limitandoci a quelle di diritto interno – che prospettano un'implementazione della sanzione penale come principale strumento di gestione del fenomeno.

2. Il diritto penale di fronte alla diffusione di notizie false *online*: i reati astrattamente configurabili.

Non è certo l'odierno allarme sociale per la circolazione delle *fake news* ad aver sollevato per la prima volta il tema del rapporto del diritto penale con la *falsità* delle notizie o delle informazioni. Invero, già nel Codice penale, così come nella legislazione complementare, sono frequenti le previsioni incriminatrici che consentono di punire la creazione o trasmissione di contenuti comunicativi non corrispondenti a verità[18]: tali fattispecie risulteranno senz'altro applicabili, ove ne siano integrati i relativi presupposti, anche alle moderne *fake news*.

In alcune ipotesi, anzitutto, la legge penale incrimina *espressamente* condotte di diffusione di informazioni false. La previsione con connotati di maggiore generalità è la contravvenzione di cui all'art. 656 c.p., che punisce con l'arresto fino a tre mesi o l'ammenda fino a 309 euro, se il fatto non costituisce più grave reato, la pubblicazione o diffusione di notizie "false, esagerate o tendenziose" atte a turbare l'ordine pubblico[19]. La nozione ampia di *diffusione*, intesa come divulgazione con qualsiasi mezzo a una pluralità di persone (a differenza della pubblicazione, che è tradizionalmente concepita in relazione alla stampa cartacea[20]), non sembra porre ostacoli a ricondurre al fatto tipico di cui all'art. 656 c.p. anche i fatti di propagazione di *fake news* attraverso i social network o le piattaforme *online*, in quanto dalle stesse possa derivare un

[15] L'esempio più noto è la (denunciata) influenza di *hacker* russi nell'elezione di Donald Trump alla presidenza americana, attraverso la diffusione di *fake news* sul conto dell'avversaria Hillary Clinton, nonché nel *referendum* britannico sulla Brexit. Per un'analisi approfondita di questi fenomeni v. Comandini (2018), pp. 199 ss., che affronta anche il tema dell'incidenza delle *fake news* sulle elezioni politiche italiane del 2018.
[16] Ancora Comandini (2018), pp. 194-195.
[17] Sul fenomeno dello *hate speech* e sul ruolo dei *social media* nella sua diffusione cfr. Abbondante (2017), p. 41 ss. V. anche Spena (2017), p. 577 ss.
[18] Perini (2017), pp. 2-6.
[19] Cfr., *ex multis*, Alessandri (1973), p. 708; Barile (1962), p. 855; Chiarotti (1964), p. 515; Giannola (2008), p. 4808; Frezza (2005), p. 4860.
[20] Chiarotti (1964), p. 515.

pericolo per l'ordine pubblico.

Peraltro, la riesumazione di tale fattispecie in vista del suo impiego nel contrasto al moderno fenomeno delle *fake news* desta più di una perplessità. Nell'impianto originario del Codice Rocco, invero, l'art. 656 c.p. assumeva una chiara impronta liberticida per la manifestazione del pensiero, essendo finalizzato a criminalizzare l'espressione di opinioni politiche sgradite al regime fascista. Ciò nonostante, la permanenza della contravvenzione nell'attuale assetto democratico è stata legittimata dalla Corte costituzionale, come avvenuto per la maggior parte degli altri reati di opinione presenti nel Codice Rocco[21], attraverso un'attività di reinterpretazione diretta a rendere l'incriminazione compatibile con la garanzia costituzionale della libertà di espressione di cui all'art. 21 Cost.

Tale ricostruzione ermeneutica ha coinvolto, in primo luogo, la determinazione del *contenuto* che le notizie devono possedere perché la loro diffusione costituisca reato: il codice penale, infatti, non si limita a incriminare le ipotesi di notizie sicuramente *false*, cioè difformi dal vero, ma prende in considerazione anche quelle meramente *esagerate*, vale a dire che contengono verità amplificate, ingigantite o iperboliche, nonché quelle *tendenziose*, in cui la realtà è presentata in modo deformato e ingannevole. È evidente come, nell'intento del legislatore fascista, il riferimento alle notizie "esagerate" e a quelle "tendenziose" costituisse il veicolo per colpire opinioni di dissenso politico. La Corte costituzionale[22], pertanto, ha precisato che le notizie tendenziose sono "quelle che, pur riferendo cose vere, le presentino tuttavia (non importa se intenzionalmente o meno) in modo che chi le apprende possa avere una rappresentazione alterata della realtà"[23], con la conseguenza che le stesse non si distinguono dalle notizie false, traducendosi comunque in una deformazione della verità[24]; nel campo di applicazione dell'art. 656 c.p., quindi, non vanno ricomprese "interpretazioni, valutazioni, commenti, ideologicamente qualificati, e persino tendenziosi, relativi a cose vere", i quali rientrano nell'ambito costituzionalmente tutelato delle libere opinioni, ma soltanto "notizie che, in un modo o nell'altro, non rappresentano il vero"[25]. L'interpretazione fornita dalla Consulta, peraltro, risulta discutibile rispetto al proposito di salvaguardare la libertà di pensiero: invero, non vi è chi non scorga l'opinabilità del discrimine tra mere interpretazioni "tendenziose" del vero e notizie "falsate" in virtù del modo in cui sono rappresentate[26].

Un secondo profilo problematico attiene alla determinazione della portata offensiva della fattispecie. L'art. 656 c.p. non incrimina le condotte di *pubblicazione* o *diffusione* in sé e per sé, in ragione della mera falsità della notizia, ma solo in quanto dalle stesse possa derivare un pericolo per l'ordine pubblico[27]: secondo la Corte costituzionale, la finalità di tutela del bene giuridico dell'ordine pubblico – questo inteso nel significato ideale di "ordine legale su cui poggia la convivenza sociale" – in quanto "immanente al sistema costituzionale", legittima la compressione della libertà di manifestazione del pensiero che può derivare dall'incriminazione delle condotte di pubblicazione o diffusione di notizie false, esagerate o tendenziose (v. *infra*, § 4), sempreché la fattispecie sia interpretata secondo lo schema del pericolo in concreto, richiedendosi che le false notizie, "in considerazione del contenuto delle medesime o delle circostanze di tempo e di luogo della diffusione stessa, risultino idonee a determinare un turbamento consistente nell'insorgenza di un completo ed effettivo stato di minaccia dell'ordine stesso" 28. Peraltro, nell'interpretazione della giurisprudenza di legittimità, l'art. 656 c.p. è per lo più configurato come un reato di pericolo astratto, per la cui sussistenza è sufficiente l'astratta possibilità di verificazione del turbamento al bene giuridico tutelato, senza che sia necessario accertarne il concreto pericolo[29]: tale orientamento finisce per obliterare del tutto l'elemento della tutela dell'ordine pubblico, rendendo penalmente perseguibile qualsiasi

[21] Per la ricostruzione di tale filone della giurisprudenza costituzionale, v. Pelissero (2010), p. 98 ss.
[22] Corte Cost., 16 marzo 1962, n. 19.
[23] Il che può avvenire, secondo la Corte, "pel fatto che vengano riferiti o posti in evidenza soltanto una parte degli accadimenti (eventualmente quelli marginali e meno importanti), sottacendone o minimizzandone altri (eventualmente di pari o maggiore importanza, o comunque idonei a spiegare o addirittura a giustificare quelli riferiti); pel fatto che gli accadimenti vengano esposti in modo da determinare confusione tra notizia e commento; e in altri simili modi".
[24] Secondo la Consulta, l'espressione "notizie false, esagerate o tendenziose" è "una forma di endiadi, con la quale il legislatore si è proposto di abbracciare ogni specie di notizie che, in qualche modo, rappresentino la realtà in modo alterato". Cfr. Giannola (2006), p. 4808.
[25] V. anche Cass. pen., 11.1.1977, in *Riv. pen.*, 1977, 463.
[26] Fumo (2018), p. 88.
[27] *Contra* Chiarotti (1964), p. 516, secondo cui bene giuridico tutelato dalla norma non sarebbe l'ordine pubblico ma la correttezza in sé dell'informazione pubblicata o diffusa.
[28] Corte Cost., 14 dicembre 1972, n. 199; 16 marzo 1962, n. 19.
[29] Cass. pen., 1.7.1996, Natola, n. 9475; Cass. pen., 4.2.1976, Catanese, in *Cass. pen. mass. ann.*, 1976, 734 con nota di Mulliri, p. 735.

espressione di pensiero giudicata non conforme alla verità "ufficiale", in tal modo accentuando la potenzialità repressiva della norma nei confronti delle opinioni avverse.

Infine, occorre considerare il profilo dell'elemento soggettivo: trattandosi di una contravvenzione, è sufficiente che l'autore sia in colpa rispetto alla falsità della notizia, in tal modo configurandosi in capo ai consociati un onere di controllo circa la correttezza e la provenienza delle informazioni diffuse (sarà, infatti, punibile chi pubblichi una notizia creduta vera senza verificare adeguatamente l'attendibilità della fonte).

In definitiva, se sul piano descrittivo la fattispecie di cui all'art. 656 c.p. si mostra idonea a coprire i fatti rientranti nel fenomeno delle *fake news*, sul piano valoriale, però, la norma continua a riflettere una concezione autoritaria dello Stato, tipica del regime fascista, prestandosi a un impiego di stampo liberticida e di repressione del dissenso politico o sociale. Prima di rispolverare l'arsenale punitivo proprio del regime fascista e di adattarlo alle esigenze contemporanee, dunque, sarebbe opportuno interrogarsi seriamente sui rischi che una simile impostazione potrebbe ingenerare.

L'art. 656 c.p. non costituisce, peraltro, l'unica disposizione originaria del Codice Rocco che si presta a essere recuperata nella repressione delle *fake news*. La clausola di sussidiarietà presente nell'art. 656 c.p. segnala che la norma assume portata residuale rispetto ad altre fattispecie incriminatrici di maggiore gravità. Più precisamente, sempre in materia contravvenzionale, la diffusione di notizie false (dunque, anche via *web*) può integrare gli estremi del procurato allarme punito dall'art. 658 c.p., relativo alla condotta di "chiunque, annunziando disastri, infortuni o pericoli inesistenti, suscita allarme presso l'Autorità, o presso enti o persone che esercitano un pubblico servizio"[30]. La fattispecie ha una portata più ristretta rispetto a quella precedentemente indicata, riguardando esclusivamente le notizie riferite a fatti idonei a suscitare allarme sociale[31].

In rapporto di specialità con l'art. 656 c.p. è pure il delitto di disfattismo politico (art. 265 c.p.), collocato tra i delitti contro la personalità dello Stato e corredato dalla previsione di pene decisamente più severe (reclusione fino a cinque anni), sebbene la sua rilevanza sia circoscritta ai tempi di guerra: la norma punisce chi "diffonde o comunica voci o notizie false, esagerate o tendenziose, che possano destare pubblico allarme o deprimere lo spirito pubblico o altrimenti menomare la resistenza della nazione di fronte al nemico"[32].

La diffusione di informazioni false assume espressa rilevanza penale anche nei delitti di aggiotaggio "informativo"[33], previsti in funzione di tutela dell'economia pubblica e del funzionamento del mercato finanziario. L'ipotesi generale, disciplinata dall'art. 501 c.p. (rubricato "Rialzo o ribasso fraudolento di prezzi sul pubblico mercato o nelle borse di commercio"), incrimina le condotte di pubblicazione o divulgazione ("comunque" realizzata) di "notizie false, esagerate o tendenziose" che siano idonee a "cagionare un aumento o una diminuzione del prezzo delle merci, ovvero dei valori annessi nelle liste di borsa o negoziabili nel pubblico mercato"[34]. Di maggiore rilevanza pratica sono le figure speciali di aggiotaggio previste dall'art. 2637 c.c. e dall'art. 185 T.U.F. (d.lgs. 24 febbraio 1998, n. 58), volte a tutelare la corretta formazione del prezzo degli strumenti finanziari: più precisamente, ai sensi dell'art. 2637 c.c. la diffusione di notizie false è incriminata nella misura in cui sia idonea "a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato"[35]; specularmente, nell'art. 185 T.U.F. (rubricato "Manipolazione del mercato") la medesima condotta informativa deve essere idonea "a provocare una sensibile alterazione del prezzo di strumenti finanziari", individuati in quelli "ammessi alle negoziazioni di un mercato regolamentato ovvero per i quali sia stata presentata domanda di ammissione"[36].

[30] La contravvenzione è punita con l'arresto fino a sei mesi o con l'ammenda da 10 a 516 euro.
[31] Ad esempio, il reato in esame è stato ravvisato rispetto alla condotta di un giornalista che aveva pubblicato la notizia di un possibile attentato al Presidente della Camera dei deputati, senza aver previamente verificato l'oggettiva attendibilità della fonte da cui aveva appreso la notizia (Cass. pen., sez. I, 20.4.2012, n. 19367). Non configura il reato, viceversa, la denuncia della scomparsa di una persona (Cass. pen., sez. I, 4.10.2017, n. 43815).
[32] Cfr. Cristiani (1964), p. 129; Aprile (2010), p. 134.
[33] L'aggiotaggio c.d. informativo, consistente nella divulgazione di notizie o informazioni, si distingue dall'aggiotaggio c.d. operativo, che incrimina altri comportamenti idonei a realizzare l'evento di pericolo, i quali possono consistere in artifizi di varia natura.
[34] Sul delitto di aggiotaggio comune cfr. Pedrazzi (1958).
[35] Mucciarelli (2002), p. 421; Seminara (2002), p. 453; Rossi (2006), p. 2637.
[36] Rossi (2006), p. 2647; Consulich (2010), pp. 297 ss. Sui rapporti con l'illecito amministrativo di manipolazione di mercato di cui all'art. 187-ter T.U.F., recentemente riformato a opera del d.lgs. 10 agosto 2018, n. 107, e le connesse problematiche in relazione al principio di *ne bis in idem* europeo (art. 4, Prot. 2 Cedu), v. per tutti Mucciarelli (2018), pp. 184 ss.

Accanto ai casi, fin qui descritti, di espressa incriminazione della diffusione di notizie false (i quali, come detto, sono agevolmente riferibili anche alla divulgazione di *fake news* tramite *internet*)[37], la legislazione penale contempla talune fattispecie in cui la falsità dell'informazione, pur non direttamente tipizzata, assume rilievo come possibile *estrinsecazione concreta* della condotta, con cui si realizza l'offesa al bene giuridico di volta in volta tutelato[38].

L'ipotesi più significativa è sicuramente il delitto di diffamazione (art. 595 c.p.), il quale può trovare applicazione rispetto all'immissione sul *web*, in modo visibile a più persone, di contenuti che, per la loro falsità, offendono la reputazione di specifici soggetti. Occorre precisare che, per l'integrazione del reato, è in via di principio irrilevante che l'addebito sia vero o falso[39], contando esclusivamente la sua capacità di ledere il bene giuridico della reputazione del soggetto passivo, inteso come dignità della persona in un dato contesto sociale[40]. Peraltro, la falsità della notizia può rilevare nel senso di escludere la possibilità per l'autore del reato di avvalersi della c.d. *exceptio veritatis*, nelle ipotesi in cui è ammessa la prova liberatoria basata sulla verità del fatto (art. 596 c.p.), nonché, in particolare, di invocare l'esimente dell'esercizio del diritto di cronaca[41], *ex* art. 51 c.p., quale estrinsecazione della libertà di manifestazione del pensiero di cui all'art. 21 Cost.: invero, la verità (*oggettiva* o, quanto meno, *putativa*[42]) del fatto esposto costituisce uno dei limiti, insieme a quelli della continenza e della pertinenza, cui la giurisprudenza subordina il diritto costituzionalmente tutelato di trasmettere informazioni lesive dell'altrui reputazione, anche questa dotata di rilevanza costituzionale ai sensi degli artt. 2 e 3 Cost.[43]

L'applicabilità del delitto di diffamazione agli autori di *fake news* offensive dell'onorabilità personale è ampiamente riconosciuta in giurisprudenza: in particolare, si è ripetutamente affermato che la pubblicazione di offese personali sia su articoli *web*[44], sia su *social network* (come *Facebook*)[45] integra l'aggravante dell'uso di un qualunque altro mezzo di pubblicità diverso dalla stampa, di cui all'art. 595, comma III, c.p., in quanto potenzialmente capace di raggiungere un numero indeterminato o comunque quantitativamente apprezzabile di persone. Tuttavia, un ostacolo alla repressione delle offese *online* discende dalla mancata estensibilità ad *internet* – in virtù del divieto di analogia *in malam partem* – della nozione di stampa di cui all'art. 1, l. 47/1948, cui consegue l'inapplicabilità dell'aggravante di cui all'art. 13 della stessa legge, nonché della responsabilità per omesso controllo *ex* art. 57 c.p. rispetto ai direttori delle testate telematiche[46]; una nozione estensiva di stampa è stata, invece, accolta dalle Sezioni Unite al fine di consentire l'applicazione *in bonam partem* alle testate telematiche registrate delle garanzie previste per gli stampati in tema di divieto di sequestro preventivo[47]. Si segnala, peraltro, che il prevalente indirizzo della giurisprudenza di legittimità in materia di art. 57 c.p., già in passato messo in discussione da alcuni giudici di merito, è stato recentemente oggetto di *revirement* ad opera di una sentenza della V sezione della Cassazione, che ha riconosciuto la responsabilità per omesso controllo in capo al direttore di un quotidiano *online*[48].

In altre ipotesi incriminatrici, collocate al di fuori della materia dei delitti contro l'onore, la condotta di diffusione di false notizie tramite *internet* può assumere rilievo penale quale pos-

[37] La comunicazione di una falsa notizia assume, altresì, rilevanza penale nelle c.d. falsità giudiziarie, tra cui i delitti di falsa denunzia o falsa incolpazione (simulazione di reato e calunnia, *ex* artt. 367 e 368 c.p.) e quelli che consistono nella violazione di un dovere di dire la verità, come la falsa testimonianza (art. 372 c.p.), le false informazioni al pubblico ministero (art. 371-bis c.p.) e le false dichiarazioni al difensore (art. 371-ter c.p.). In ragione degli specifici soggetti cui devono essere dirette le informazioni non veritiere, tuttavia, è difficile (se non del tutto impossibile, nel caso dei delitti che ruotano intorno al nucleo della falsa testimonianza) ipotizzare l'integrazione di tali reati attraverso la diffusione di notizie via *internet*.

[38] Per questa distinzione v. Perini (2017), p. 5.

[39] Padovani (2014), p. 273.

[40] Sull'evoluzione dottrinale e giurisprudenziale della nozione di reputazione (dalla concezione fattuale, a quella normativa a quella personalistica e costituzionale), v. per tutti Musco (1974), *passim*; Siracusano (1993), pp. 33 ss.; Gullo (2013), pp. 11 ss.; Gullo (2015), pp. 189 ss.

[41] Questo può essere definito come diritto di informare la collettività tramite il mezzo della stampa su accadimenti di pubblico interesse: cfr. Musco (1990), p. 645.

[42] Gullo (2013), p. 32; Id. (2016), p. 4.

[43] Tali criteri sono stati enucleati sin dalla nota sentenza sul c.d. "decalogo dei giornalisti" della Cassazione civile del 1984 (Cass. civ., sez. I, 18.10.1984, n. 5259).

[44] Cass. pen., sez. V, 15.10.2018, n.57020.

[45] *Ex multis*, Cass. pen., sez. I, 28.4.2015, n. 24431.

[46] Cass. pen., sez. V, 16 luglio 2010, n. 35511; Cass. pen., sez. V, 29 novembre 2011, n. 44126. In tema v. Seminara (2014), p. 584 ss.; Petrini (2017), p. 1485 ss.

[47] Sez. Un., 17 luglio 2015, n. 31022, su cui v. Gullo (2016).

[48] Cass. pen., 23 ottobre 2018, n. 1275, pubblicata su *Diritto penale contemporaneo* (online), 28 febbraio 2019, con nota di Mauri.

sibile strumento di realizzazione di un *inganno* ai danni della vittima (nella specie, l'internauta che viene in contatto con la *fake news*). Questo accade, in modo paradigmatico, nel delitto di truffa (art. 640 c.p.), in cui la condotta di "artifizi o raggiri" potrebbe essere integrata dalla pubblicazione su un *social network* di una notizia decettiva (es. una falsa raccolta di fondi da destinare in beneficienza), che induca la vittima a compiere un atto di disposizione patrimoniale a sé sfavorevole, con corrispondente profitto del creatore della bufala o di terzi intermediari.

Prima della depenalizzazione operata dal d.lgs. 8/2016, una forma di inganno penalmente rilevante, anche nella forma meramente tentata, era quella configurata dalla contravvenzione di pericolo dell'abuso della credulità popolare (art. 661 c.p.), che puniva con l'arresto sino a tre mesi o con l'ammenda sino a 1032 euro chiunque, pubblicamente, cercasse "con qualsiasi impostura, anche gratuitamente, di abusare della credulità popolare", sempre che dal fatto potesse derivare "un turbamento dell'ordine pubblico". È evidente come tale fattispecie avrebbe potuto attagliarsi anche a numerosi casi di *fake news*, specificamente finalizzate a far presa sulla credulità degli utenti di internet per fini di profitto (si pensi al fenomeno, sopra descritto, del *click-baiting*).

L'inganno rileva, altresì, ai sensi dell'art. 294 c.p. ("Attentato contro i diritti politici dei cittadini"), quale mezzo attraverso cui sia impedito "in tutto o in parte l'esercizio di un diritto politico" (ad esempio, i diritti di elettorato attivo e passivo) ovvero si determini taluno "a esercitarlo in senso difforme dalla sua volontà". Si potrebbe riflettere sull'applicabilità di tale fattispecie alle ipotesi di *fake news* costruite ad arte al fine di manipolare le opinioni dei cittadini in periodo di campagna elettorale e a indirizzarne il voto verso determinate forze politiche: la punibilità potrebbe, però, ravvisarsi solo in casi estremi, in quanto la norma non incrimina semplici suggestioni, ma richiede il realizzarsi di un vero e proprio inganno ai danni del cittadino, mediante l'impiego di mezzi fraudolenti equiparabili alla violenza e alla minaccia "in ordine all'idoneità ad esercitare sull'elettore una pressione di tale intensità da indurlo a determinarsi nell'esercizio di un diritto politico in modo contrario alla sua reale volontà"[49]. Quand'anche consentita sul piano del dato testuale della norma, peraltro, un'interpretazione dell'art. 294 c.p. che consenta di reprimere le *fake news* c.d. "politiche" potrebbe rivelarsi pericolosa, in quanto suscettibile di un utilizzo strumentale rispetto alla repressione di opinioni avverse, con evidente *vulnus* per i principi di democrazia e di libertà di pensiero. Anche qui, dunque, come a proposito della contravvenzione di cui all'art. 656 c.p., può ribadirsi la forte perplessità rispetto all'idea di recuperare nella "lotta alle *fake news*" fattispecie incriminatrici che recano ancora chiara l'impronta dell'originaria impostazione codicistica di repressione del dissenso politico.

2.1. (segue) *Diritto penale e verità della notizia.*

Dall'esame delle fattispecie astrattamente applicabili alla diffusione di notizie false tramite *internet* è possibile trarre alcune considerazioni generali sulla *verità* quale possibile oggetto di tutela penale (la "cura penale della verità", per usare un'espressione di Pulitanò[50]). L'attribuzione di rilevanza penale alle *fake news* presuppone, infatti, l'idea che a determinate condizioni il diritto possa imporre un "dovere di dire la verità" penalmente sanzionato.

Non è questa la sede per discutere sul problema *ontologico* della verità, cioè della sua esistenza e della possibilità di una sua definizione[51]. Il diritto penale, nell'incriminare condotte variamente riconducibili al concetto di falsità, muove dall'implicito presupposto che una realtà oggettiva esista e che questa possa essere oggetto di rappresentazione nell'intelletto umano (*adaequatio intellectus et re*[52]). Il diritto penale, nella sua dimensione sostanziale, prescinde anche dal profilo *epistemologico* della verità, relativo all'*an* e al *quomodo* della sua conoscibilità che, tuttavia, assume rilievo nel momento dell'accertamento giudiziale (c.d. verità processuale, la quale è sempre verità "relativa", cioè valevole solo ai fini del processo[53]). Peraltro, la prospettiva

[49] Cass. pen., sez. I, 26.6.1989, in *Dejure*. Nella specie, veniva esclusa la configurabilità del delitto rispetto a un discorso svolto nel corso di una trasmissione televisiva e contenente l'espressione dello scarso interesse per i quesiti sottoposti a *referendum* abrogativo e, al contrario, il preminente interesse per il problema della caccia rimasto estraneo alla consultazione referendaria del novembre 1987.
[50] Pulitanò (2014), p. 87. Sul tema v. anche Padovani (2014), pp. 17 ss.
[51] Häberle (2000), p. 40 ss.
[52] È la definizione che di "verità" dà Tommaso d'Aquino, nelle sue *Quaestiones disputatae de veritate*.
[53] Ferrua (2017), p. 31 ss.; Ferrajoli (1989), p. 40 ss.

processuale consente di evidenziare i limiti all'intelligibilità del *vero* in senso metafisico, di cui il legislatore dovrebbe essere consapevole nel momento in cui compie scelte di criminalizzazione. Ciò è ancor più vero per i reati aventi a oggetto la comunicazione di proposizioni falsamente rappresentative della realtà, nei quali la verità deve essere accertata a un duplice livello: quello dell'esistenza del fatto narrato (c.d. verità ontica), e quello della corrispondenza dell'enunciato al fatto che esso rappresenta (c.d. verità semantica)[54].

Il problema più delicato, però, attiene alla concezione della verità quale possibile oggetto di tutela penale. In primo luogo, occorre osservare che uno specifico *obbligo di verità* può configurarsi solo rispetto alle fattispecie in cui è espressamente incriminata una condotta di falso (si pensi ai delitti contro la fede pubblica, alla falsa testimonianza o alle ipotesi in cui la legge penale attribuisce rilievo, a vario titolo, alla diffusione di notizie false). Anche in questi casi, peraltro, il falso non assume rilievo in sé e per sé, ma solo in quanto sia dotato di un'oggettiva *idoneità ingannatoria*, vale a dire sia potenzialmente idoneo a indurre in errore i destinatari della dichiarazione o della cosa cui si riferisce. Nelle ipotesi in cui il disvalore del fatto tipico è polarizzato sull'evento di inganno (ad es., nella truffa), invece, la condotta assume rilevanza penale a prescindere dal suo contenuto di falsità, ma solo in quanto effettivamente determini una falsa rappresentazione nel destinatario, cioè lo induca in errore: qui la legge penale non impone un obbligo di dire il vero, e la falsità viene unicamente in considerazione come possibile strumento di inganno[55].

In ogni caso, può osservarsi che nell'attuale assetto punitivo l'incriminazione della diffusione di notizie false è sempre correlata al carattere decettivo della condotta (in quanto *idonea a* ingannare ovvero *causativa* di inganno). Ciò si spiega con il fatto che la verità non viene mai tutelata *in quanto tale* dal diritto penale, come bene giuridico protetto in via diretta e immediata dalla singola fattispecie, ma solo in funzione strumentale rispetto alla protezione di interessi ulteriori, che possono essere lesi dalla divulgazione di notizie false (ad es., l'ordine pubblico nell'art. 656 c.p.; il funzionamento del mercato nei delitti di aggiotaggio)[56]: il diritto penale non vuole proteggere un interesse astratto alla conoscenza della verità metafisica delle cose, ma reputa che, in talune circostanze, l'affermazione di falsità o la propagazione di notizie false possa comportare un pericolo per specifici beni giuridici individuali o collettivi.

Spesso, tuttavia, il rapporto tra la *verità* dell'informazione e l'*interesse ulteriore* tutelato dalla norma diviene inafferrabile e evanescente. Si pensi, in particolare, al caso del c.d. negazionismo, che nel nostro ordinamento ha rilevanza penale *sub specie* di circostanza aggravante dei reati di propaganda razzista, di istigazione e di incitamento di atti di discriminazione commessi per motivi razziali, etnici, nazionali o religiosi, attualmente disciplinati dall'art. 604-bis c.p.[57]: tale fattispecie prevede una cornice autonoma di pena (da due a sei anni) per i casi in cui "la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale". Nell'aggravante del negazionismo, quindi, viene in considerazione un'ipotesi peculiare di *falsa notizia*, relativa alla negazione di fatti storici ritenuti di particolare gravità (il genocidio degli ebrei durante la Seconda guerra mondiale e altri crimini internazionali); la circostanza, peraltro, potrebbe essere integrata anche dalla pubblicazione o dalla diffusione di *fake news* "storiche" mediante la rete. Senza addentrarci nell'esame della norma e delle questioni connesse alla sua legittimazione, in particolare con riferimento al principio della libertà di pensiero[58], quel che preme qui evidenziare è il fatto che, a differenza di quanto osservato per le ipotesi incriminatrici precedentemente esaminate, in tal caso è più vaga l'individuazione degli interessi cui possa ritenersi finalizzata la "tutela della verità": nonostante il legame causale con la condotta discriminatoria del reato base, infatti, non sembra che il maggior disvalore connesso all'aumento di pena si fondi sull'offesa alla dignità e alla sensibilità personale del soggetto passivo della discriminazione (ad esempio in quanto appartenente al gruppo sociale vittima di genocidio); l'aggravamento del carico sanzionatorio potrebbe, al più, correlarsi alla lesione dell'insieme dei valori etici attorno a cui si riconoscono

[54] Fiorelli (2018), p. 6.
[55] Padovani (2014), p. 23 ss.
[56] Perini (2017), p. 3.
[57] La norma è stata inserita dal d.lgs. n. 21/2018, in attuazione della c.d. riserva di codice. L'aggravante, introdotta con la l. 115/2016, era precedentemente regolata al comma 3-bis, l. 654/1975.
[58] Si rimanda, per tutti, a Puglisi (2016), p. 21 ss.; Fronza (2016), p. 1031 ss.

le società democratiche, i quali sarebbero pericolosamente minacciati da chi disconosca la verificazione dei fatti storici che di quei valori costituiscono la più radicale negazione[59]. In tal modo, però, si postula una concezione etica dello Stato, il quale si pone come depositario dei valori "giusti" da perseguire e si arroga il diritto di incriminare le espressioni ideologiche difformi: una concezione, questa, del tutto antitetica all'idea laica e pluralista che dovrebbe informare l'assetto di una società democratica, di cui la libertà di espressione – estesa a tutte le forme di pensiero, *anche antidemocratiche* – costituisce una delle principali estrinsecazioni e garanzie di sopravvivenza.

Come si dirà a breve, nella direzione di esasperare il valore della *verità della notizia* in quanto tale, quale bene tutelato a prescindere dalla protezione di interessi ulteriori (o in vista della protezione di beni di estrema vaghezza), sembrano muoversi anche alcune delle recenti proposte normative in tema di criminalizzazione delle *fake news*. Più in generale, il tema della tutela penale della verità si traduce in un problema di *offensività* della singola fattispecie incriminatrice: si tratta di capire, cioè, se l'intervento penale contro condotte di falsità sia giustificato dalla necessità di proteggere un bene che sia effettivamente meritevole di tutela. Tale valutazione di meritevolezza, a sua volta, non può che essere condotta mediante un bilanciamento con la garanzia costituzionale della libertà di espressione del pensiero (art. 21 Cost.), la cui compressione può essere giustificata solo in vista della protezione di un bene di preminente rilevanza costituzionale (v. *infra*, § 4).

3. *Fake news* e nuove istanze di incriminazione.

Alla luce dell'inquadramento del fenomeno delle *fake news* all'interno dell'attuale assetto normativo, è possibile svolgere alcune considerazioni *de lege ferenda*.

In primo luogo, sarebbe erroneo ritenere che con lo sviluppo di *internet* e dei *social media* siano emerse esigenze di tutela del tutto *nuove*, che non possano essere soddisfatte con gli strumenti del diritto penale tradizionale. Invero, pur in assenza di previsioni incriminatrici specifiche, la pressoché totalità dei casi di propagazione di menzogne tramite *social media* può già essere agevolmente ricompresa nella descrizione tipica di fattispecie che, in vario modo, conferiscono rilevanza penale alle condotte di diffusione di false notizie. In particolare, come si è visto, oltre ad ipotesi che attribuiscono rilievo a *specifici contenuti* di falsità informativa (economica, storica, diffamatoria, ecc.), il codice penale contempla una norma di carattere generale – la contravvenzione di pubblicazione e diffusione di notizie false, esagerate o tendenziose, di cui all'art. 656 c.p. – che consente di estendere la punibilità a qualsiasi tipo di *fake news*, purché astrattamente idoneo a turbare l'ordine pubblico: quest'ultimo, peraltro, costituisce un limite estremamente vago, sia per l'indeterminatezza della nozione di ordine pubblico[60], di cui è discussa la capacità di fungere da elemento selettivo di condotte penalmente rilevanti[61]; sia per la (invero, ormai risalente) costruzione giurisprudenziale della fattispecie secondo lo schema della pericolosità in astratto (v. *supra*), che consente di prescindere dall'accertamento della concreta messa in pericolo del bene giuridico tutelato. Inoltre, come si è già avuto modo di osservare, pare fortemente discutibile il riferimento a questo e altri modelli punitivi che esprimono lo spirito liberticida dello Stato fascista, non essendo auspicabile il recupero in chiave moderna di prospettive repressive per la libertà di manifestazione del pensiero.

Del tutto prive di rilevanza penale rimarrebbero, ad ogni modo, quelle *fake news* rispetto a cui non sia possibile rinvenire un collegamento, nemmeno potenziale, con la lesione dell'ordine pubblico: vi potrebbero rientrare, oltre alle notizie su argomenti del tutto ininfluenti, che non destano particolare preoccupazione, le false informazioni su argomenti politici, la cui diffusione su larga scala può creare un rischio di inquinamento del dibattito pubblico e di manipolazione delle opinioni degli elettori. In questa prospettiva, lo sviluppo dei *social media* avrebbe evidenziato una lacuna di tutela rispetto a quello che potremmo definire, in termini generalissimi, il "bene giuridico della democrazia", cioè l'interesse al funzionamento democratico dello Stato e alla corretta formazione del pensiero politico dei cittadini. È su questo

[59] Macchia (2019), p. 22 ss.
[60] Sulla nozione di ordine pubblico, nella duplice accezione "ideale" e "materiale", v. per tutti, Fiore (1980), p. 1084 ss.; De Vero (1995), p. 76 ss.
[61] Moccia (1990), p. 1 ss.

aspetto che, come si vedrà, insistono particolarmente le principali proposte legislative. Va detto, in senso fortemente critico rispetto alla prospettiva di criminalizzazione, che il problema della distorsione dell'informazione a fini propagandistici e di condizionamento dell'opinione pubblica non è un fenomeno necessariamente correlato alla diffusione di contenuti sulle piattaforme *online*, le quali semmai ne hanno aggravato l'impatto in termini quantitativi[62]. Inoltre, anticipando considerazioni che si riprenderanno in seguito (v. *infra*, § 5), suscita perplessità l'idea di un intervento penale a tutela di un bene giuridico dai contorni incerti come quello democratico, che potrebbe piuttosto veicolare la repressione di manifestazioni di dissenso politico, spingendosi addirittura oltre l'impianto repressivo originario del Codice Rocco.

Con riferimento alle ipotesi già coperte dallo strumento penale, il problema che si pone è, semmai, quello dell'inadeguatezza del trattamento sanzionatorio delle fattispecie esistenti rispetto alle esigenze di tutela evidenziate dall'utilizzo di internet. In particolare, la contravvenzione di cui all'art. 656 c.p. si rivela di scarsissima utilità pratica, in ragione delle pene del tutto irrisorie da essa previste (in via alternativa, l'arresto fino a tre mesi o l'ammenda fino a 309 euro). La risposta sanzionatoria risulta, invece, maggiormente efficace nelle ipotesi in cui la diffusione di notizie false integri il delitto di diffamazione, ovvero una fattispecie contro il patrimonio (ad es., la truffa) o contro l'economia pubblica o il mercato finanziario (delitti di aggiotaggio).

A fronte di tali premesse, le principali proposte di riforma che contemplano l'utilizzo dello strumento penale in funzione di contrasto alle *fake news* possono raggrupparsi lungo due direttrici: da un lato, si suggerisce di estendere la punibilità rispetto a comportamenti in precedenza penalmente irrilevanti; dall'altro, si propone di incidere in senso peggiorativo sul trattamento sanzionatorio di fattispecie esistenti, al fine di accentuarne la capacità dissuasiva sul piano della "minaccia di pena".

3.1. *Il disegno di legge "Gambaro".*

A partire dalla fine della precedente legislatura, sulla spinta dell'affiorare improvviso del dibattito sulle *fake news* a livello di opinione pubblica, si è assistito a un'autentica proliferazione di progetti di legge volti ad arginare il fenomeno in esame attraverso l'utilizzo della norma penale. Si tratta di iniziative che, pur rimaste per il momento sulla carta[63], rappresentano in modo significativo le preoccupazioni e le istanze punitive emergenti nella società, come dimostra il ricorrente ripresentarsi del tema delle *fake news* nel discorso giornalistico e politico[64]. Tali istanze, inoltre, travalicano la dimensione nazionale trovando un'eco nelle legislazioni *anti-fake* news proposte o approvate da altri Paesi europei[65] o nelle iniziative assunte a livello di Unione europea[66].

Tra le proposte di legge presentate al Parlamento italiano, quella senz'altro più significativa, anche per le reazioni che ha suscitato tra gli interpreti, è il c.d. d.d.l. Gambaro (A.S. 2688) del 7 febbraio 2017, recante "Disposizioni per prevenire la manipolazione dell'informazione *on line*, garantire la trasparenza sul *web* e incentivare l'alfabetizzazione mediatica"[67].

[62] Zanon (2017), p. 3 ss.

[63] La maggior parte delle proposte sono relative alla scorsa legislatura. Tuttavia, anche nell'attuale legislatura sono state presentate due proposte di legge in argomento (entrambe depositate alla Camera dei Deputati il 31 ottobre 2018), di cui però non sono ancora stati pubblicati i testi: si tratta degli atti AC 1325, Minardo, "Norme per regolamentare il funzionamento delle piattaforme di comunicazione e delle comunità virtuali nella rete internet" e AC 1328, Pastorino, "Istituzione dell'Osservatorio nazionale per il monitoraggio della rete internet". Di recente, inoltre, è stata presentata una richiesta di istituzione di una "Commissione di inchiesta sulla diffusione intenzionale e massiva di informazioni false attraverso la rete internet e sul diritto all'informazione e alla libera formazione dell'opinione pubblica" (AC 1056, Fiano e altri).

[64] Da ultimo, il problema delle *fake news* è stato sollevato con riferimento al rischio di inquinamento delle elezioni per il Parlamento europeo che si svolgeranno nel prossimo mese di maggio: cfr. Marro, *Fake news, come possono influenzare le prossime elezioni europee*, ne *Il Sole 24 Ore* (online), 25 febbraio 2019.

[65] Significativa, in particolare, la legge tedesca: *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* (Netzwerkdurchsetzungsgesetz – NetzDG), n. 536/17, 30 giugno 2017. Al momento, anche in Francia sono in discussione due proposte di legge sulle false informazioni durante il periodo elettorale (n. 799 del 21 marzo 2018 e n. 772 del 16 marzo 2018).

[66] Il Parlamento europeo ha approvato una risoluzione il 23 novembre 2016 sulla comunicazione strategica dell'UE per contrastare la propaganda nei suoi confronti da parte di terzi. Nel 2018, la Commissione europea ha incentivato la firma di un codice di autoregolamentazione da parte di piattaforme digitali (Facebook, Google e Mozilla) per contrastare la disinformazione *online*: si tratta del c.d. *Code of Practice on Disinformation*, su cui v. Monti (2019), p. 320.

[67] La dottrina ha accolto tale disegno di legge in senso profondamente critico. V. Fumo (2018), p. 88; Melzi d'Eril (2017), p. 62; Cuniberti (2017), p. 31; Guercia (2019), p. 1258.

Già dalla Relazione introduttiva traspare un atteggiamento culturale di forte preoccupazione, se non addirittura timore, nei confronti del fenomeno delle *fake news*, che viene descritto con toni quasi apocalittici: si legge, ad esempio, che "con il diffondersi dei *social media* il pericolo di contaminare *internet* con notizie inesatte e infondate o, peggio ancora, con opinioni che seppur legittime rischiano di apparire più come fatti conclamati che come idee, è in crescita esponenziale"; e ancora, "se il pubblico di internet prende per buono e fondato qualsiasi cosa circoli *online*, senza più distinguere tra vero e falso, il pericolo è enorme". Per converso, gli autori della proposta minimizzano il rischio che dalla previsione di forme di controllo sulla circolazione di notizie in rete potrebbe derivare per la libertà di espressione: quest'ultima, invero, "non può trasformarsi semplicemente in un sinonimo di totale mancanza di controllo, laddove controllo, nell'ambito dell'informazione, vuol dire fornire una notizia corretta a tutela degli utenti".

La demonizzazione dei *social media* quale strumento di propaganda antidemocratica si traduce, sul piano della risposta penale, nella previsione di nuove fattispecie incriminatrici. In generale, si osserva come l'ampliamento dell'area del penalmente rilevante passa attraverso il rimodellamento di tipi di incriminazione propri del Codice Rocco, già fortemente connotati sul piano valoriale come reati di opinione, che vengono ulteriormente sviluppati in senso repressivo. In maggior dettaglio, l'art. 1 del progetto, riprendendo la contravvenzione di cui all'art. 656 c.p., introduce nel codice penale l'art. 656-*bis*, rubricato "Pubblicazione o diffusione di notizie false, esagerate o tendenziose, atte a turbare l'ordine pubblico, attraverso piattaforme informatiche", diretta a punire con l'ammenda fino a 5.000 euro, e sempre che il fatto non costituisca più grave reato, chiunque "pubblica o diffonde, attraverso piattaforme informatiche destinate alla pubblicazione o diffusione di informazione presso il pubblico, con mezzi prevalentemente elettronici o comunque telematici, notizie false, esagerate o tendenziose che riguardino dati o fatti manifestamente infondati o falsi". La contravvenzione si pone in rapporto di specialità con l'art. 656 c.p., almeno sotto due profili: i) in relazione al *contenuto delle notizie* "false, esagerate o tendenziose", con precisazione difficilmente comprensibile, si prevede che queste debbano avere a oggetto "dati o fatti manifestamente infondati o falsi"; ii) in relazione alle *modalità della condotta* di pubblicazione o diffusione, si specifica che questa può realizzarsi esclusivamente mediante strumenti informatici o telematici. Tale seconda limitazione è particolarmente significativa, nella misura in cui sottende l'idea di un maggior disvalore, e dunque di una maggiore meritevolezza di pena, nel comportamento di chi divulghi notizie false tramite *internet* rispetto a chi utilizzi strumenti diversi. Ciò si ricollega alla previsione, contenuta nell'ultimo comma dell'art. 1, di una causa personale di esclusione di punibilità per i giornalisti professionisti[68], quasi che la diffusione di notizie false, tendenziose o esagerate sia meno grave (rientrando nella previsione generale di cui all'art. 656 c.p.) quando promani da soggetti qualificati; come è stato rilevato, però, si tratta di una premessa infondata, essendo semmai vero il contrario, in quanto la narrazione di un fatto falso da parte di un giornalista di professione, qualsiasi sia il mezzo utilizzato (stampa cartacea, televisione, radio o piattaforma telematica), è suscettibile di trarre in inganno il lettore più facilmente di una *fake news* diffusa da fonti anonime o poco attendibili sui *social network*, in virtù della maggiore credibilità tradizionalmente riposta nei confronti degli esercenti la professione giornalistica[69].

L'aspetto che maggiormente colpisce nel testo dell'art. 656-*bis* c.p. è l'attribuzione di rilevanza penale alla falsità in sé del fatto narrato, senza richiedere che dalla condotta derivi un'offesa per un interesse ulteriore, neppure nella forma della mera messa in pericolo[70]. Sotto questo profilo, si rileva un'incongruenza tra la rubrica dell'articolo, che contiene il riferimento al pericolo di turbamento per l'ordine pubblico, sulla falsariga dell'art. 656 c.p., e il testo della fattispecie, che invece pare tutelare la *verità della notizia* in quanto tale. Si tratta di un'impostazione che, per le concezioni eticizzanti e assolutistiche che evoca, pare di difficile legittimazione alla luce del principio di offensività.

Accanto alla fattispecie contravvenzionale in oggetto, il d.d.l. Gambaro propone di introdurre due ulteriori ipotesi delittuose che rimarcano lo schema del disfattismo politico (art. 265 c.p.) e ne estendono la punibilità al tempo di pace: più precisamente, con il nuovo art.

[68] A norma dell'art. 1, ultimo comma, del d.d.l., l'art. 656-bis non si applica ai "soggetti e ai prodotti di cui alla legge 8 febbraio 1948, n. 47, e di cui all'articolo 1, comma 3-bis, della legge 7 marzo 2001, n. 62".
[69] Melzi d'Eril (2017), p. 62. Anche Cuniberti (2017), p. 33 segnala il paradosso di riservare un trattamento di favore nei confronti di una categoria che, al contrario, dovrebbe essere gravata da maggiori doveri di responsabilità.
[70] Bassini e Vigevani (2017), p. 15.

265-*bis* c.p. ("Diffusione di notizie false che possono destare pubblico allarme, fuorviare settori dell'opinione pubblica o aventi ad oggetto campagne d'odio e campagne volte a minare il processo democratico") si andrebbero a punire, anche con la pena detentiva (reclusione non inferiore a dodici mesi, congiuntamente ad un'ammenda fino a 5000 euro), le condotte di diffusione o comunicazione di "voci o notizie false, esagerate o tendenziose, che possono destare pubblico allarme", nonché quelle aventi a oggetto lo svolgimento di "un'attività tale da recare nocumento agli interessi pubblici o da fuorviare settori dell'opinione pubblica, anche attraverso campagne con l'utilizzo di piattaforme informatiche destinate alla diffusione *online*"; con il successivo art. 265-*ter* c.p. ("Diffusione di campagne d'odio o volte a minare il processo democratico") dovrebbe punirsi ancor più severamente (con la reclusione non inferiore a due anni e con l'ammenda fino a 10000 euro), "ai fini della tutela del singolo e della collettività", chiunque si renda responsabile "anche con l'utilizzo di piattaforme informatiche destinate alla diffusione *online*, di campagne d'odio contro individui o di campagne volte a minare il processo democratico, anche a fini politici".

Entrambe le fattispecie risultano carenti sotto il profilo della tassatività e determinatezza, in quanto si connotano per l'estrema vaghezza nella descrizione della condotta (ad es. "qualsiasi attività") e, soprattutto, nell'individuazione dell'oggetto di tutela, rispetto a cui dovrebbe prodursi l'evento di danno: difficile capire cosa si intenda per "recare nocumento agli interessi pubblici", o per "minare il processo democratico, anche a fini politici"[71]. Al di là della genericità della formulazione, può poi osservarsi come in tali reati emerga una duplice prospettiva di tutela: quella personalistica, soprattutto nell'incriminazione delle "campagne d'odio contro individui" (il fenomeno del c.d. *hate speech* che, come si è detto *supra*, § 1, è spesso correlato a quello delle *fake news*); e quella pubblicistica, riferita al bene della "democrazia" in senso lato, declinato nella corretta formazione dell'opinione pubblica e nel regolare svolgimento del "processo democratico". La valorizzazione di quest'ultimo profilo è molto preoccupante, perché assegna alla norma penale forti valenze di repressione politica, secondo una logica ancor più oppressiva di quella che aveva connotato le scelte del codificatore in epoca fascista: qualsiasi attività di manifestazione del pensiero è potenzialmente in grado di recare un nocumento a un "interesse pubblico", o di "fuorviare settori dell'opinione politica", ed è evidente il rischio di trasformare la norma penale in uno strumento di contrasto rispetto alle notizie "scomode" o alle opinioni espressive di ideologie contrarie a quelle dominanti in un dato contesto storico-politico, mediante la loro etichettatura come "false" o semplicemente "tendenziose".

La tendenza repressiva si riflette anche sulla severità del trattamento sanzionatorio, che contempla addirittura il ricorso alla pena detentiva, in modo del tutto sproporzionato rispetto al disvalore delle condotte sanzionate. Peraltro, la fissazione del solo limite edittale inferiore (reclusione "non inferiore a" – rispettivamente – dodici mesi o due anni) comporta la determinazione della pena massima, per effetto dell'integrazione automatica *ex* art. 23 c.p., in ventiquattro anni: è giusto il caso di evidenziare l'assoluta abnormità di tale divaricazione edittale, che esporrebbe la norma a sicure censure di incostituzionalità sotto i profili della determinatezza e della proporzionalità della pena.

3.2. *Le altre proposte di legge.*

In direzione simile al d.d.l. Gambaro si muove un ulteriore disegno di legge presentato durante la scorsa legislatura (A.S. 2689/2017[72]), volto alla "Introduzione degli articoli 656-*bis*, 656-*ter* e 656-*quater* del codice penale in materia di pubblicazione o diffusione di notizie false dirette a danneggiare il diritto all'immagine degli eletti nelle istituzioni rappresentative". Anche in questo caso si prevede un'implementazione dello strumento punitivo in funzione di tutela dei meccanismi di funzionamento delle istituzioni democratiche, sul presupposto di una loro messa in pericolo tramite la propagazione di *fake news* sulla rete. Più precisamente, un nuovo art. 656-*bis* c.p. dovrebbe punire, anche con pena detentiva (arresto fino a tre mesi, in alternativa all'ammenda fino a 309 euro), la pubblicazione o diffusione di "notizie false, esagerate o tendenziose, riguardanti eletti nelle istituzioni rappresentative, per le quali possa essere recato danno al godimento del diritto alla propria immagine, alla tutela dell'identità

[71] Fumo (2018), p. 88.
[72] Presentato al Senato in data 7 febbraio 2017.

personale, del proprio buon nome, della buona reputazione e credibilità in sé". Si tratta, quindi, di un'ipotesi speciale di diffamazione, caratterizzata dalla qualità di eletto in capo al soggetto passivo. È prevista una circostanza aggravante per l'eventualità in cui "la pubblicazione avvenga mediante l'utilizzo di tecnologie dell'informazione e della comunicazione che permetta la loro diffusione su reti sociali virtuali".

Il riferimento alle *fake news* è immediatamente visibile nel successivo art. 656-*ter* c.p., che punisce con le stesse pene "chiunque pubblica o diffonde notizie false, esagerate o tendenziose mediante l'utilizzo di tecnologie dell'informazione e della comunicazione che permetta la loro diffusione su reti sociali virtuali, *con il fine di influenzare e arrecare danno al buon andamento della politica democratica della Repubblica*". La pena è, poi, raddoppiata nel caso in cui la pubblicazione avvenga durante i periodi di campagna elettorale. Si osserva che qui il danno al "buon andamento della politica democratica della Repubblica", pur denotando il bene giuridico tutelato dalla fattispecie, rileva esclusivamente quale requisito finalistico della condotta, costituendo oggetto di dolo specifico, mentre non si richiede la sua effettiva realizzazione sul piano oggettivo. A proposito di tale elemento, possono reiterarsi (e pure con maggiore intensità) le osservazioni critiche già formulate in merito all'art. 265-bis c.p. ipotizzato dal Progetto Gambaro, con riferimento all'indeterminatezza del bene giuridico tutelato e alla sua evidente connotazione sul piano della repressione del dissenso politico: è chiaro che qualunque condotta di "diffusione di notizie" (vere o false che siano) può ritenersi indirizzata a "influenzare" il buon andamento della politica democratica della Repubblica, sicché la previsione penale si trasforma in uno strumento di censura di qualunque espressione ideologica di dissenso politico, al di fuori di qualsiasi possibilità legittimazione sul piano costituzionale.

Il disegno di legge in oggetto prevede, da ultimo, l'introduzione di un nuovo art. 656-*quater* c.p., avente a oggetto la pubblicazione o diffusione di notizie false, tendenziose o esagerate "con il fine di indurre all'odio, a comportamenti violenti o di propaganda terroristica"; la pena è raddoppiata in caso di realizzazione del fatto tramite *internet*. Anche in questo caso la norma non richiede l'accertamento di una concreta pericolosità della condotta, limitandosi a caratterizzare la diffusione di notizie sul piano dell'elemento soggettivo; ed è, quindi, di nuovo evidente il rischio di piegamento della norma penale in funzione di repressione di opinioni ideologiche percepite come ostili dal potere costituito.

Tra i progetti di intervento penale contro le *fake news* si segnala, infine, la proposta di legge De Maria (A.C. 4557/2017)[73]. Tale testo propone di modificare la fattispecie contravvenzionale di cui all'art. 656 c.p., sia mediante l'ampliamento della condotta tipica sia mediante l'inasprimento del trattamento sanzionatorio. Più precisamente, nella nuova formulazione il reato dovrebbe contenere l'espresso riferimento alla realizzazione del fatto "anche mediante l'utilizzo della rete telefonica o attraverso strumenti telematici o informatici"; inoltre, le notizie false, esagerate o tendenziose possono essere idonee, oltre che al turbamento dell'ordine pubblico, anche "ad arrecare danno ingiusto alle persone". Così formulato, però, il reato potrebbe porre problemi di coordinamento con il tentativo di truffa. Sotto il profilo sanzionatorio, il nuovo art. 656 c.p. sarebbe punito con la "reclusione da tre mesi a cinque anni", trasformandosi conseguentemente in ipotesi delittuosa. È, infine, prevista una circostanza aggravante "se il fatto è commesso per fini di lucro, ovvero se le notizie riguardano atti di violenza a sfondo razziale, sessuale o comunque di natura discriminatoria".

4. La diffusione di false notizie nel quadro dei reati di opinione: il limite della libertà di manifestazione del pensiero.

Nel riflettere sulla legittimazione e sull'opportunità di un intervento punitivo in funzione di contrasto al fenomeno delle *fake news*, non può prescindersi dall'esame del ruolo che, in questa materia, svolge la libertà di espressione del pensiero garantita dall'art. 21 della Costituzione.

Punto di partenza imprescindibile del discorso è capire se la comunicazione di contenuti informativi *falsi* possa essere, o meno, compreso nella sfera protettiva del principio costituzionale in esame. In primo luogo, si ritiene che il "pensiero" tutelato dall'art. 21 Cost. non sia

[73] Proposta presentata alla Camera dei deputati il 15 giugno 2017.

soltanto l'*opinione*, cioè la formulazione di un giudizio teoretico o fattuale[74], ma anche l'affermazione circa l'esistenza o l'inesistenza di fatti[75]: e questo vale a prescindere dalla difficoltà (secondo alcuni, l'impossibilità[76]) di scindere concettualmente le opinioni dalla pura e semplice esposizione di avvenimenti. In secondo luogo, dalla lettura del testo della Costituzione non sembra che possa ricavarsi una limitazione della libertà di espressione sulla base del *contenuto* del pensiero manifestato: l'art. 21 Cost. garantisce la manifestazione di *qualunque* pensiero, e dunque giusto o sbagliato, corretto o insensato, eticamente accettabile o aberrante, *vero* o *falso* che sia.

L'interpretazione che qui si propone non sembra condivisa da tutta la dottrina costituzionalistica: alcuni autori[77] ritengono che la tutela costituzionale della libertà di manifestazione del pensiero non possa estendersi al "subiettivamente falso" (quali sono "la menzogna, il dolo, l'inganno, il raggiro, o la frode"), limitandosi a coprire "l'obiettivamente erroneo"; in termini differenti si esprimeva altra autorevole dottrina[78], secondo cui "neppure la diffusione di notizie false può essere considerata illecita in sé e per sé" e "il fine d'inganno può essere illecito solo in quanto costituisca il fulcro di un'attività illecita che contrasti con altri principi costituzionali".

La seconda impostazione convince maggiormente. Infatti, dire che l'art. 21 Cost. si estende a tutelare le manifestazioni dichiarative *indipendentemente dal loro contenuto di veridicità* non significa escludere che le stesse possano, in taluni casi e a certe condizioni, essere oggetto di incriminazione: la protezione costituzionale ha la funzione di impedire che i comportamenti di falso siano puniti *in sé*, a prescindere dalla loro capacità di incidere su altri interessi maggiormente meritevoli di tutela (es. la pubblica fede nei delitti contro la fede pubblica)[79]. L'interpretazione estensiva della libertà di espressione diviene ancor più necessaria se si considera la difficoltà di capire cosa sia vero e cosa sia falso, per cui si rivelerebbe illusoria la pretesa di individuare il discrimine della tutela costituzionale alla luce di un criterio indeterminato come quello della verità; del pari, come si è già accennato, non sempre è agevole distinguere l'esposizione di un *fatto* falso dall'espressione di un'*opinione* erronea o infondata.

Dunque, anche il "pensiero falso", cioè la narrazione di fatti non corrispondenti al vero (o, ed è lo stesso, l'inesatta rappresentazione di fatti veri), rientra nella tutela costituzionale di cui all'art. 21 Cost. Ne consegue che i reati mediante i quali è punita la trasmissione di informazioni o di dati falsi dovrebbero essere ricompresi nella categoria dei reati di opinione, intesi nel significato ampio di fattispecie che incriminano la manifestazione di un pensiero[80]: anche rispetto a tali ipotesi si pone, quindi, il problema della compatibilità con la libertà di espressione.

Sulla base di tali premesse, occorre chiedersi se la compressione del diritto di manifestare liberamente il proprio pensiero, che conseguirebbe all'incriminazione delle *fake news*, possa ritenersi giustificata dall'esigenza di tutelare un interesse *di rilevanza costituzionale* e *di preminente importanza* rispetto alla libertà di espressione. Per la corretta applicazione del principio del bilanciamento tra interessi costituzionali confliggenti, infatti, non basta che la fattispecie penale sia prevista a protezione di un interesse che trovi riferimento, anche implicito, nella Costituzione; occorre invece che quell'interesse possa dirsi prevalente rispetto alla libertà di espressione[81]: si tratta di una prospettiva che, pur talvolta obliterata dalla giurisprudenza costituzionale interna in materia di delitti politici[82], dovrebbe essere adeguatamente valorizzata anche alla luce delle indicazioni elaborate dalla Corte europea dei diritti dell'uomo nell'interpretazione dell'art. 10 Cedu posto a protezione della libertà di espressione[83].

[74] Per la distinzione tra critica teoretica e fattuale v. Pelissero (1992), p. 1228.
[75] Sul punto v. Lehner (2019), p. 108, e *ivi* il rimando a C. Cost., 13.7.1960, n. 59.
[76] Secondo Fois (1957), p. 202, la narrazione dei fatti implica pur sempre un'attività di tipo valutativo (quanto meno in relazione alla scelta degli argomenti e delle modalità espositive); altri Autori evidenziano l'influenza delle percezioni soggettive e delle categorie interpretative personali sull'esposizione dei fatti, che quindi non può mai dirsi davvero oggettiva: v. per tutti Barile (1975), p. 3.
[77] A partire da Esposito (1958), p. 37 ss.; in questo senso v. anche Pace e Manetti (2006), pp. 89-90.
[78] Barile (1984), p. 229.
[79] Si noti, peraltro, che nonostante la differente premessa teorica, a tale conclusione perviene anche Esposito (1958), pp. 36-37.
[80] Così Pelissero (2015), p. 38, che riconduce a tale categoria, oltre ai reati di opinione politici, anche i reati a tutela delle confessioni religiose, i reati di apologia di genocidio e di discriminazione razziale, etnica e religiosa, l'aggravante di negazionismo, nonché i delitti di ingiuria e diffamazione. Cfr. anche Spena (2007), p. 697 ss.
[81] In caso contrario, come scrive magistralmente Fiore (1972), p. 89, "della libertà di espressione non rimarrebbe veramente niente, visto che non c'è quasi nessun bene-interesse della vita individuale o collettiva, a cui la Costituzione non faccia in qualche modo riferimento". Su questo profilo v. anche Pelissero (2015), p. 39, che ricollega la necessità di valutare l'importanza dei beni costituzionali in conflitto alla giurisprudenza della Corte europea dei diritti dell'uomo in tema di art. 10 Cedu.
[82] Cfr. Pelissero (2015), p. 38 e giurisprudenza costituzionale *ivi* citata.
[83] C. Edu, *Perinçek c. Svizzera* [Grande Camera], ric. n. 27510/08, 15.10.2015

Orbene, per quanto la valutazione circa l'importanza dei beni di volta in volta tutelati spetti alla discrezionalità del legislatore, sembra potersi escludere che i beni giuridici messi in pericolo dalla diffusione di *fake news* siano tali da rendere opportuno l'intervento penale, con conseguente sacrificio della libertà di espressione. Sicuramente insostenibile è l'idea prospettata dal Progetto Gambaro di incriminare la diffusione di notizie false "in sé", cioè a prescindere dalla lesione di interessi ulteriori (v. *supra*, § 3.1.): nell'attuale assetto costituzionale pluralista, la verità, comunque la si consideri, non può assurgere al rango di interesse dotato di rilievo costituzionale[84]. Diversamente, la punibilità è tendenzialmente legittimata in presenza di beni di carattere personalistico (come la reputazione individuale): ciò è dimostrato dalla giurisprudenza che individua la verità del fatto come limite all'esercizio del diritto di cronaca, a sua volta espressione della libertà di manifestazione del pensiero. La prospettiva individualistica, peraltro, è scarsamente presa in considerazione dai progetti di riforma, trattandosi di esigenze di tutela già soddisfatte dalle norme esistenti in tema di diffamazione.

Il nodo più problematico attiene alla legittimazione dell'intervento penale rispetto alla diffusione di notizie che prevedono un pericolo per l'ordine pubblico o per la corretta formazione del dibattito democratico. Con riferimento all'ordine pubblico, può ricordarsi di nuovo (v. *supra*, § 2) come la Corte costituzionale, nel lontano 1962, abbia "salvato" dall'incostituzionalità l'art. 656 c.p., affermando che la stessa non comporta un'illegittima restrizione alla libertà di espressione in quanto "la tutela costituzionale dei diritti, come quello cui ha riguardo l'art. 21 Cost., ha sempre un limite non derogabile nell'esigenza che attraverso il loro esercizio non vengano sacrificati beni anche essi voluti garantire dalla Costituzione, e che tale deve ritenersi non solo la tutela del buon costume, cui l'articolo stesso fa espresso riferimento, ma anche il mantenimento dell'ordine pubblico, che è da intendere come ordine legale su cui poggia la convivenza sociale"[85]. In tale risalente pronuncia, tuttavia, la Corte non opera un effettivo bilanciamento dell'ordine pubblico con la libertà di diffondere informazioni, limitandosi a rilevare la copertura costituzionale dello stesso. Il richiamo alla generica nozione di ordine pubblico (quantomeno, nella dimensione "ideale" di "ordine legale costituito") non pare legittimare il sacrificio della libertà di espressione, che assume valore preminente: sotto questo profilo, la dubbia compatibilità costituzionale dell'art. 656 c.p. dovrebbe dissuadere sia dall'idea di riutilizzarlo in funzione di contrasto alle *fake news*, sia di introdurne versioni "restaurate" mediante l'ampliamento della condotta tipica o il rafforzamento sul piano sanzionatorio (v. *supra*, §§ 3.1. e 3.2). Parimenti, il sacrificio della libertà di pensiero a fronte dell'incriminazione della diffusione di *fake news* non parrebbe giustificata neppure ove fosse valorizzata la lesione di altri beni giuridici, ad esempio l'incolumità pubblica, la quale viene messa a repentaglio da alcune falsità circolanti in materia tecnico-scientifica (si pensi alla campagna anti-vaccini, con i pericoli che ne derivano per la salute collettiva): anche in questo caso, tuttavia, l'utilizzo della sanzione penale, oltre a rivelarsi scarsamente efficace, potrebbe risultare ancor più pericolosa della minaccia che intende contrastare, a causa della difficoltà di discriminare tra autentiche menzogne e semplici opinioni che, pur non validate dalla comunità scientifica, hanno comunque legittimazione a essere espresse e comunicate.

Ancora più vago e indeterminato è il riferimento, variamente declinato nelle diverse proposte di legge, al bene della "democrazia". Da questo punto di vista, se è vero che la diffusione di notizie false tramite la Rete può pericolosamente inquinare il dibattito democratico e orientare il voto dell'opinione pubblica, è anche vero che la selezione delle condotte penalmente rilevanti sulla base di tale bene giuridico potrebbe risultare ancor più pericolosa, in ragione dell'estrema genericità del concetto di democrazia e delle strumentalizzazioni politiche cui potrebbe essere piegato. Questi rischi sono tanto più evidenti se si considera, ancora una volta, il carattere sfumato della linea di demarcazione tra vero e falso (e, quindi, la difficoltà dell'accertamento demandato al giudice): se in alcuni casi le menzogne sono facilmente smascherabili (si pensi alla *fake news* sulla nascita di Obama in Kenya), in altri casi l'accertamento del fatto oggetto della notizia è molto più complesso, sicché la ricostruzione di una narrazione in termini di verità o di falsità risulta fortemente opinabile.

[84] Melzi d'Eril (2017), p. 64.
[85] C. Cost., 16.3.1962, n. 19.

5. Rilievi conclusivi: l'uso simbolico del diritto penale nella repressione del "pensiero ostile".

Le considerazioni da ultimo sviluppate consentono di evidenziare come la prospettiva di incriminazione delle *fake news*, per quanto dichiaratamente concepita in funzione di difesa della democrazia, potrebbe concretamente tradursi in un complessivo abbassamento del livello di garanzia assicurato alla libertà di manifestare e diffondere le proprie idee, la quale a sua volta costituisce il presupposto per il corretto funzionamento dei meccanismi democratici. Se il fine perseguito è quello di impedire la circolazione di notizie false, il risultato raggiunto potrebbe essere quello di introdurre surrettiziamente un controllo penale sulle attività di informazione *online* e sulle opinioni che circolano in rete. In altre parole, la sanzione penale potrebbe tramutarsi, da strumento di tutela della democrazia, in mezzo di repressione di contenuti, più che falsi, "ostili" o portatori di valori contrastanti con quelli condivisi dalla collettività: una prospettiva, questa, sicuramente incompatibile con la natura pluralista degli ordinamenti democratici.

In questo senso, le recenti istanze di criminalizzazione delle *fake news* possono essere idealmente inquadrate entro la recente tendenza legislativa al "recupero" dell'originaria connotazione dei reati di opinione quali strumenti di repressione e controllo delle manifestazioni di dissenso politico e sociale. Tracce di tale tendenza si rinvengono nella recente legislazione penale in tema di discriminazione razziale, di negazionismo, oltre che nella previsione di numerose ipotesi speciali di apologia (ad esempio, l'aggravante dell'apologia di delitti di terrorismo o crimini contro l'umanità di cui all'art. 414, ultimo comma, c.p., inserito dal d.l. 144/2005 conv. in l. n. 155/2005; oppure il delitto di pubblica apologia di pratiche di pedofilia e pedopornografia, *ex* art. 414-bis, comma 2, c.p., introdotto dalla l. 172/2012).

Nelle proposte di legge che si sono analizzate, il legislatore riscopre i meccanismi liberticidi propri del Codice Rocco e, addirittura, va oltre le scelte di incriminazione del regime fascista, in senso ancor più marcatamente e apertamente repressivo verso le espressioni di dissenso ideologico e politico. Reciso il pur labile collegamento con l'ordine pubblico, si vorrebbe adesso incriminare *qualunque* ipotesi di diffusione di notizie false o tendenziose, purché ciò avvenga attraverso i nuovi strumenti informatici, o purché l'attività di propagazione sia diretta a "influenzare" l'opinione pubblica o a ledere un interesse vagamente definito come "democratico", in tal modo aprendo la strada a forme pervasive di controllo penale sulle attività di informazione.

Non solo, poi, l'uso dello strumento penale nel contrasto alle *fake news* potrebbe comportare un rischio per la libertà d'espressione; ma è anche discutibile che lo stesso possa risultare efficace rispetto all'obiettivo di limitare la diffusione di false notizie sulla rete. Il problema principale della scarsa effettività del diritto penale rispetto a fatti commessi *online*, infatti, non deriva dalla mancanza di fattispecie incriminatrici, ma dalla difficoltà di individuare gli autori delle notizie, spesso coperti dietro l'anonimato; peraltro, non è pensabile far ricadere la responsabilità penale sugli utenti dei *social network*, che si limitano a condividere sui loro profili innumerevoli *fake news* nella evidente convinzione che siano vere notizie (a meno di ipotizzarne una responsabilità a titolo di colpa, sufficiente per la previsione contravvenzionale di cui all'art. 656 c.p.).

L'unico effetto tangibile che potrebbe derivare dalla previsione di sanzioni (non solo di carattere penale), a carico sia degli utenti sia dei gestori delle piattaforme *online* su cui trovano pubblicazione i contenuti, è che il timore della punizione disincentivi la circolazione di notizie, spingendo a forme di auto-censura e paralizzando, così, l'attività di informazione sul *web* (c.d. *chilling effect*).

In conclusione, il rischio che si avverte è quello che l'incriminazione delle *fake news* persegua scopi meramente simbolici, cioè sia volta a placare le preoccupazioni diffuse nella società, e amplificate dai *media* tradizionali, relative al ruolo distorsivo per l'informazione delle nuove tecnologie, senza tuttavia fornire una risposta efficace e giustificata sul piano delle garanzie costituzionali. Di per sé, la moltiplicazione dei centri di produzione delle notizie, non più riservate a un ristretto oligopolio informativo, costituisce una potenzialità per la libertà d'informazione e per il pluralismo democratico, assecondando il modello espresso dalla metafora di origine americana del *marketplace of ideas*. Il condizionamento dell'opinione pubblica tramite la manipolazione dell'informazione non è un fenomeno nuovo: semplicemente, sono mutate

le dimensioni e la percezione sociale del problema. I nuovi (innegabili) pericoli legati alla diffusione di *fake news* non vanno combattuti sul piano del diritto penale, che deve preservare la sua funzione di *extrema ratio*, ma attraverso rimedi di natura extra-penale, di recupero della credibilità delle fonti di informazione e, soprattutto, sul piano culturale.

Bibliografia

Abbondante, Fulvia (2017), "Il ruolo dei *social network* nella lotta all'*hate speech*: un'analisi comparata fra l'esperienza statunitense e quella europea", in *Informatica e diritto*, 1-2, pp. 41-68.

Alessandri, Alberto (1973), "Osservazioni sulle notizie false, esagerate o tendenziose", in *Rivista italiana di diritto e procedura penale*, p. 908.

Allcott, Hunt e Gentzkow, Matthew (2017), "Social Media and Fake News in the 2016 Election", in *Journal of Economic Prospectives*, vol. 31 (2), pp. 211-236.

Aprile, Ercole (2010), "Sub art. 265 c.p.", in Lupo, Ernesto e Lattanzi, Giorgio (a cura di), "Codice penale. Rassegna di giurisprudenza e di dottrina", vol. 6, Milano, Giuffrè, pp. 134-139.

Barile, Paolo (1962), "La libertà di espressione del pensiero e le notizie false, esagerate e tendenziose", in *Foro italiano*, I, p. 855.

Barile, Paolo (1975), "Libertà di manifestazione del pensiero", Milano, Giuffrè.

Barile, Paolo (1984), "Diritti dell'uomo e libertà fondamentali", Bologna, Il Mulino.

Bassini, Marco e Vigevani, Giulio Enea (2017), "Primi appunti su fake news e dintorni", in *Rivista di diritto dei media*, 1, pp. 11-22.

Comandini, Vincenzo Visco (2018), "Le *fake news* sui social network: un'analisi economica", in *Rivista di diritto dei media*, 2, pp. 183-212.

Consulich, Federico (2010), "La giustizia e il mercato. Miti e realtà di una tutela penale dell'investimento mobiliare", Milano, Giuffrè.

Chiarotti, Franco (1964), "Diffusione o pubblicazione di notizie false o tendenziose", in *Enciclopedia del diritto*, vol. XII, Milano, Giuffrè, p. 515.

Cristiani, Antonio (1964), "Disfattismo politico e economico", in *Enciclopedia del Diritto*, vol. XIII, Milano, Giuffrè, p. 129.

Cuniberti, Marco (2017), "Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo", in *Rivista di diritto dei media*, 1, pp. 26-40.

De Gregorio, Giovanni (2017), "The *market place of ideas* nell'era della post-verità: quali responsabilità per gli attori pubblici e privati online?", in *Rivista di diritto dei media*, 1, pp. 91-105.

De Vero, Giancarlo (1995), "Ordine pubblico (Delitti contro l')", in *Digesto delle discipline penalistiche*, vol. IX, Torino, Utet, pp. 72-96.

Esposito, Carlo (1958), "La libertà di manifestazione del pensiero nell'ordinamento italiano", Milano, Giuffrè.

Ferrajoli, Luigi (1989), "Diritto e ragione. Teoria del garantismo penale", Roma-Bari, Laterza.

Ferrua, Paolo (2017), "La prova nel processo penale", vol. 1, Torino, Giappichelli.

Fiore, Carlo, (1980), "Ordine pubblico (diritto penale)" (voce), in *Enciclopedia del diritto*, XXX, Milano, 1980, p. 1084 ss.

Fiorelli, Giulia (2018), "La declaratoria di *immutatio veri* nel processo penale", Torino, Giappichelli.

Fioriglio, Gianluigi (2016), "Contro la post-verità: il pluralismo assiologico quale limite del potere e garanzia della giustizia nello Stato costituzionale", in *Nomos*, 3, pp. 1-19.

Fois, Sergio (1957), "Principi costituzionali e libera manifestazione del pensiero", Milano, Giuffrè.

Frezza, Federico (2005), "Sub art. 656 c.p.", in Padovani, Tullio (a cura di), "Codice penale", Milano, Giuffrè, p. 4860.

Fronza, Emanuela (2016), "Criminalizzazione del dissenso o tutela del consenso. Profili critici del negazionismo come reato", in *Rivista italiana di diritto e procedura penale*, 2, pp. 1016-1033.

Fumo, Maurizio (2018), "Bufale elettroniche, repressione penale e democrazia", in *Rivista di diritto dei media*, 1, pp. 83-92.

Giannola, Umberto (2008), "sub Art. 656", in Dolcini, Emilio e Marinucci, Giorgio (a cura di), "Codice penale commentato", vol. II, Milano, 2006, p. 4808.

Guercia, Pierluigi (2019), "I progetti di legge sulle fake news e la disciplina tedesca a confronto", in Cadoppi, Alberto e Canestrari, Stefano (a cura di), "Cybercrime. Diritto e procedura penale dell'informatica", Wolters Kluwer, pp. 1254-1272.

Gullo, Antonio (2013), "Diffamazione e legittimazione dell'intervento penale. Contributo a una riforma dei delitti contro l'onore", Roma, Aracne editrice.

Gullo, Antonio (2015), "Delitti contro l'onore", in Piergallini, Carlo e Viganò, Francesco (a cura di), "Reati contro la persona", Estratto dal VII volume del "Trattato teorico-pratico di diritto penale" diretto da Palazzo, Francesco e Paliero, Carlo Enrico, Torino, Giappichelli, pp. 141-237.

Gullo, Antonio (2016), "Diffamazione e pena detentiva", in *Diritto penale contemporaneo* (online), 13 marzo, pp. 1-12.

Häberle Peter (2000), "Diritto e verità", Torino, Einaudi.

Lehner, Eva (2019), "Fake news e democrazia", in R*ivista di diritto dei media*, 1, pp. 93-122.

Macchia, Alberto (2019), "Spunti in tema di negazionismo", in *Cassazione penale*, 2019, pp. 22-31.

Melzi D'Eril, Carlo (2017), "Fake news e responsabilità: paradigmi classici e tendenze incriminatrici", in *Rivista di diritto dei media*, 1, pp. 60-67.

Mocanu, Delia, Rossi, Luca, Zhang, Quian, Karsai, Marton, Quattrociocchi, Walter, (2015), "Collective attention in the age of mis-information", in *Computers in human behaviour*, 51, 1198-1204.

Moccia, Sergio (1990), "Ordine pubblico (disposizioni a tutela del)" (voce), in *Enciclopedia del diritto*, XXII, Roma, p. 1 ss.

Monti, Matteo (2017), "Fake news e social network: la verità ai tempi di Facebook", in *Rivista di diritto dei media*, 1, pp. 80-90.

Monti, Matteo (2019), "Il *Code of Practice on Disinformation* dell'UE: tentativi in fieri di contrasto alle *fake news*", in Rivista di diritto dei media, 1, pp. 320-334.

Mucciarelli, Francesco (2002), "Aggiotaggio", in Alessandri, Alberto (a cura di), "Il nuovo diritto penale delle società", Milano, 2002, p. 421.

Mucciarelli, Francesco (2018), "Gli abusi di mercato riformati e le persistenti criticità di una tormentata disciplina", in *Diritto Penale Contemporaneo*, *Rivista trimestrale*, 3, pp. 174-189.

Musco, Enzo (1974), "Bene giuridico e tutela dell'onore", Milano, Giuffrè.

Musco, Enzo (1990), "Stampa (dir. pen.)" (voce), in *Enciclopedia del diritto*, vol. XLIII, Milano, 1990, p. 645.

Pace, Alessandro e Manetti, Michela (2006), "Art. 21", in Branca, Giuseppe e Pizzorusso, Alessandro (a cura di), "Commentario della Costituzione", Bologna, 2006.

Padovani, Tullio (2014), "Menzogna e diritto penale", Pisa, Pisa University Press.

Pariser, Eli (2012), "The Filter Bubble: What the Internet Is Hiding From You", New York, Penguin Books.

Pedrazzi, Cesare (1958), "Problemi del delitto di aggiotaggio", Milano.

Pelissero, Marco (1992), "Diritto di critica e verità dei fatti", in *Rivista italiana di diritto e procedura penale*, 3, pp.1227-1237.

Pelissero, Marco (2010), "Reati contro la personalità dello Stato e contro l'ordine pubblico", Torino, Giappichelli.

Pelissero, Marco (2015), "La parola pericolosa. Il confine incerto del controllo penale del dissenso", in *Questione giustizia*, 4, pp. 37-46.

Perini, Chiara (2017), "*Fake news* e post-verità tra diritto penale e politica criminale", in *Diritto penale contemporaneo* (online), 20 dicembre, pp. 1-14.

Petrini, Davide (2017), "Diffamazione on line: offesa recata con "altro mezzo di pubblicità" o col mezzo della stampa?", in *Diritto penale e processo*, 11, pp. 1485-1492.

Pinelli, Cesare (2017), "Postverità, verità e libertà di manifestazione del pensiero", in *Rivista di diritto dei media*, 1, pp. 41-47.

Pitruzzella, Giovanni (2017), "La libertà di informazione nell'era di Internet", in Pitruzzella, Giovanni, Pollicino, Oreste, Quintarelli, Stefano, "Parole e potere – Libertà d'espressione, *hate speech* e *fake news*", Milano, Egea, pp. 55-98.

Puglisi, Giuseppe (2016), "A margine della c.d. "aggravante di negazionismo": tra occasioni sprecate e legislazione penale simbolica", in Diritto penale contemporaneo (online), 15 luglio 2016, pp. 1-36.

Pulitanò, Domenico (2014), "Cura della verità e diritto penale", in Forti, Gabrio, Varraso, Gianluca, Caputo, Matteo (a cura di), "Verità del precetto e della sanzione penale alla prova del processo", Napoli, Jovene.

Rossi, Alessandra (2006), "Le fattispecie penali di aggiotaggio e manipolazione del mercato (artt. 2637 cod. civ. e 185 d. lgs. 58/98): problemi e prospettive", in Dolcini, Emilio e Paliero, Carlo Enrico, "Studi in onore di Giorgio Marinucci", vol III, Milano, Giuffrè, pp. 2637-2673.

Savarese, Paolo (2018), "Dalla bugia alla menzogna: la postverità e l'impossibilità del diritto", in *Nomos*, 2, pp. 1-21.

Seminara, Sergio (2002), "L'aggiotaggio", in Seminara, Sergio e Giarda, Angelo, "I nuovi reati societari: diritto e processo", Padova, 2002, p. 453.

Seminara, Sergio (2014), "Internet (diritto penale)" (voce), in *Enciclopedia del diritto*, Annali VII, Milano, 2014, pp. 584 ss.

Siracusano, Placido (1993), "Ingiuria e diffamazione" (voce), in *Digesto delle discipline penalistiche*, vol. VIII, Torino, Utet, p. 32.

Spena, Alessandro (2007), "Libertà di espressione e reati di opinione", in *Rivista italiana di diritto e procedura penale*, 2-3, pp. 689-738.

Spena, Alessandro (2017), "La parola(-)odio. Sovraesposizione, criminalizzazione e interpretazione dello *hate speech*", in *Criminalia*, pp. 577-607.

Sunstein, Cass (2014), "On Rumors: How Falsehoods Spread, Why We Believe Them and What can be Done", Princeton.

Zanon, Nicolò (2018), "*Fake news* e diffusione dei *social media*: abbiamo bisogno di un'Autorità pubblica della Verità?" (2018), in *Rivista di diritto dei media*, 1, pp. 1-5.

Il volto dei reati di opinione nel contrasto al terrorismo internazionale al tempo di *Internet*

El rostro de los delitos de opinión en la lucha contra el terrorismo internacional en la época de Internet

The Face of Word Crimes in the Fight Against International Terrorism at the Time of the Internet

Paolo Cirillo
Dottorando di ricerca in diritto penale presso l'Università degli Studi di Napoli "Federico II"
paolo.cirillo2@unina.it

Principio di legalità | Principio de legalidad | Nullum crimen principle

Abstracts

Negli ultimi anni la rinascita della categoria dei reati di opinione si è manifestata in modo significativo nel settore dell'antiterrorismo. In tale contesto, in cui il pensiero islamico radicale assume un ruolo nevralgico e l'utilizzo degli strumenti di comunicazione di massa un carattere catalizzatore, alla nuova vita delle fattispecie d'opinione hanno contribuito tutti i formanti della sistematica penalistica: forme legislative di tutela anticipata, *inputs* sovranazionali di criminalizzazione ed ermeneutiche giudiziarie flessibilizzanti.
Il sistema che ne deriva, fatto di delitti svincolati da valutazioni di offensività e di dubbia compatibilità con la libertà di manifestazione del pensiero, si presta a evidenti censure di costituzionalità: almeno con riferimento ai principi – recentemente valorizzati anche nell'ottica sovranazionale – di determinatezza/prevedibilità e di proporzionalità del ricorso alla pena.
È l'ennesima prova di come, nella lotta al terrorismo, il – pur irrinunciabile – diritto penale perda i suoi connotati garantistici per accostarsi ad un paradigma, se non "del nemico", quantomeno "al limite".

En los últimos años, la categoría de los delitos de opinión ha resurgido de manera significativa en el ámbito de la lucha contra el terrorismo. El pensamiento islámico radical y los nuevos medios de comunicación explican en buena medida este fenómeno. Todos los actores relevantes del derecho penal han contribuido a la revitalización de los delitos de opinión: el legislador, los órganos jurisdiccionales internos y el sistema supranacional. El sistema resultante, compuesto por delitos no relacionados con declaraciones ofensivas y de difícil compatibilidad con la libertad de expresión, plantea serios interrogantes respecto de su constitucionalidad: al menos con respecto a los principios - recientemente valorados también en el sistema supranacional - de previsibilidad de la condena penal y proporcionalidad de la pena. Esto demuestra cómo, en la lucha contra el terrorismo, el derecho penal - aunque indispensable - pierde sus connotaciones de garantía para acercarse, en mayor o menor medida, a un paradigma de "derecho penal del enemigo".

Recently the category of word crimes has reappeared significantly in the area of counter-terrorism. In this context, the radical islamic thought acquires a nerve-wracking role and the new media have a core character. All the actors of the criminal law have contributed to the revival of word crimes: both the domestic legislator and the internal courts and the supranational system. The resulting system, made up of crimes unrelated to offensive evaluations and of doubtful compatibility with the freedom of expression, shows clear censorships of constitutionality: at least with reference to the principles - recently valued also in the supranational system – of predictability of criminal

conviction and proportionality of the penalty. It is the proof of how, in the fight against terrorism, the - indispensable - criminal law loses its characteristics of guarantee to approach a paradigm "of the enemy".

Sommario

1. La (ri)emersione dei reati di opinione.

Negli ultimi anni, è tornato alla ribalta, sia pure in chiave moderna, il tema dei reati di opinione[1].

Un tema che, dopo i toni dell'accesa polemica degli Autori degli anni settanta in relazione al coevo terrorismo politico-istituzionale, sembrava essersi quasi del tutto sottratto alle luci dei riflettori[2], anche a fronte della scarsa applicazione pratica che queste fattispecie ricevevano.

Il silenzio sull'argomento, durato diversi decenni, era stato interrotto solamente dalla riforma disorganica e non del tutto soddisfacente del 2006, varata nel tentativo di riallineare la materia ai principi costituzionali del diritto penale[3].

Da allora, per una sorta di eterogenesi dei fini, si è assistito, piuttosto che al definitivo declino dei reati di opinione, ad una loro silenziosa rinascita.

Inevitabilmente, la loro (ri)emersione ha (ri)proposto l'aporia – già lucidamente evidenziata da John Stuart Mill[4] – tra tutela della sicurezza collettiva, a cui tali delitti sono ispirati, e autonomia politica individuale, su cui il nostro ordinamento giuridico costituzionale si fonda.

Si tratta, con tutta evidenza, di una contraddizione di cui il sistema non riesce a liberarsi. Il contrasto è ancora vivo ed emerge, ritornando d'attualità, rispetto ad una pluralità di materie: dalla nuova aggravante di negazionismo introdotta nel 2016[5]; ai reati di istigazione e apologia previsti dal 2012 in materia di pedofilia e violenza sessuale coinvolgenti minori di età (art. 414-*bis* c.p.); fino ad arrivare alle recenti proposte – di cui ciclicamente si discute in Parlamento – finalizzate alla criminalizzazione dei recrudescenti fenomeni omofobi[6], così come, più in generale, degli *hate speeches* e, ancora, dei rigurgiti di propaganda nazi-fascista[7].

1.1. *La materia antiterrorismo e il ruolo di* Internet.

In questo quadro composito è stata soprattutto la materia dell'antiterrorismo ad aver fatto registrare la riemersione dei reati di opinione.

Questi delitti ben s'inseriscono tra le diverse figure anticipatorie della soglia d'intervento penale che caratterizzano la tutela progressiva su cui è costruito l'odierno diritto penale di contrasto al terrorismo internazionale, esempio d'avanguardia di "sub sistema repressivo *off-shore*"[8].

Al cospetto del terrorismo globale i reati di opinione presentano, accanto alla loro tradizionale portata problematica, aspetti inediti propri del fenomeno e connessi alle dinamiche del tempo presente.

Da un lato, in tale contesto le condotte di diffusione del pensiero assumono un ruolo nevralgico per la profonda connessione che esiste tra il pensiero islamico radicale ed il fenomeno

[1] La denominazione "reati di opinione", ancorché tradizionalmente adottata e particolarmente efficace sul piano comunicativo, sarebbe impropria. Cfr. Spena (2007), p. 689 ss. il quale rileva che non s'incrimina un mero atto di pensiero, come suggerirebbe la lettera della locuzione; piuttosto, occorre la manifestazione/espressione di un certo contenuto di pensiero. Si propone, perciò, di sostituire la denominazione, per una maggiore aderenza alle modalità esecutive del comportamento e al principio penalistico di materialità, con quella di "reati di espressione". In questi termini, si vedano anche: Di Giovine (1988), p. 16; Bognetti (1971), p. 55.

[2] Fiore (1972). Più di recente, per una ricostruzione del sistema dei reati di opinione cfr. Alesani (2006); Pulitanò (2006), p. 239 ss.; Visconti (2008); Pelissero (2010), p. 95 ss.

[3] In senso critico sulla novella n. 85 del 2006, cfr. Padovani (2006), p. 23 ss.; Pelissero (2006), p. 1197 ss.; Clemente (2007), p. 26-33.

[4] Stuart Mill (2000), p. 105 ss.

[5] Il riferimento è alla legge n. 115 del 16 giugno 2016 che, già emendata dalle legge europea del 2017, inserisce un nuovo comma 3 *bis* nella legge n. 654 del 1975. Per un'analisi dell'aggravante, cfr. Scotto Rosato (2016), p. 292 ss.

[6] Il riferimento è al disegno di legge 245 del 13 marzo 2013, immediatamente archiviato, e al disegno di legge 1052 del 19 settembre 2013, approvato alla Camera e poi arenatosi al Senato. Sulla tematica cfr. Dolcini (2014), p. 7 ss.

[7] Il riferimento è alla proposta di legge 3343 (c.d. Fiano) volta all'introduzione all'art. 293-*bis* c.p. concernente il reato di propaganda del regime fascista e nazifascista, approvata alla Camera il 12 settembre 2017 e poi arenatasi in Senato.

[8] Paliero (2012), p. 115.

terroristico *tout court*, per cui il primo è nucleo essenziale e giustificazione del secondo.

Dall'altro lato, la capacità diffusiva del terrorismo islamista ha trovato un supporto nelle nuove tecnologie e nei moderni strumenti di comunicazione di massa. In particolare, *internet* e *social media* sono divenuti i canali principali usati dai terroristi per le proprie attività: tant'è vero che si parla di un autonomo *cyber Caliphate* formato da "nativi digitali" di cui è impossibile assicurare un controllo capillare[9].

Mentre i fenomeni terroristici del passato fondavano le proprie attività su approcci diretti e personali, la peculiarità del jihadismo militante dei nostri giorni è il sapiente e massiccio utilizzo di tutti i più moderni strumenti tecnologici[10].

La destrutturazione del nuovo terrorismo internazionale, privo di gerarchie stabili, trova il suo referente nella flessibilità e globalità del mondo virtuale.

La strategia mediatica messa in campo punta tanto sui *social network*, accessibili in tempo reale e senza filtro da utenti di tutto il mondo, quanto sulle più classiche pubblicazioni telematiche.

Ne derivano una serie di vantaggi, un tempo impensabili, per la diffusione dei messaggi estremisti; le radicalizzazioni, infatti, diventano ampie e diffuse, nonché immediate e sostanzialmente incontrollabili, in grado di conquistare, a distanza e spesso segretamente, soggetti conosciuti e sconosciuti.

La forza travolgente dei *new media* è tale che si sono individuate diverse funzioni che gli estremisti perseguono con l'utilizzo di tali canali, a cui si affiancano le recenti innovazioni tecnologiche (*smartphones*, *tablets*): dalla propaganda *erga omnes* degli obiettivi e dei risultati delle singole strutture terroristiche, alla pubblica intimidazione; dal reclutamento e dall'indottrinamento, alla vera e propria diffusione di materiali volti all'addestramento; dall'organizzazione, anche a distanza, degli episodi terroristici, fino alla rivendicazione e all'elogio delle condotte realizzate dallo stesso agente o da terzi[11].

Si tratta, in buona sostanza, di un "cerchio" che, chiudendosi su se stesso, rappresenta l'ossatura delle dinamiche dell'isalmismo militante.

Sul terreno criminologico appena delineato si innesta la nuova vita dei reati di opinione, frutto del contributo dei diversi formanti della scienza penalistica, preoccupata di apprestare strumenti quanto più incisivi possibili per contrastare il fenomeno in tutte le sue fasi: fattispecie legislative a tutela anticipata, *inputs* sovranazionali di criminalizzazione ed ermeneutiche giudiziarie flessibilizzanti.

2. Il formante legislativo.

Di fronte all'allarme del terrorismo internazionale è stato, innanzitutto, il legislatore ad intervenire: prima, arricchendo il codice penale di nuove fattispecie incriminatrici; poi, ritoccando le medesime.

Il risultato è stato una radicale innovazione dell'intero compendio delittuoso.

Quest'ultimo, fino a quel momento storico, aveva assunto una caratterizzazione essenzialmente interna, calibrato sul solo terrorismo nazionale-politico dei c.d. "anni di piombo". In verità, già allora il Titolo I del Libro II del codice penale, di per sé a forte connotazione ideologica, era divenuto la sede principale della legislazione dell'emergenza e della prevalenza delle istanze della politica sulle garanzie individuali.

A partire dagli anni duemila, si è proseguiti su questa strada, introducendo una serie, nutrita e complessa, di illeciti, pronta a subire modifiche in aderenza al carattere fortemente evolutivo e sempre *in fieri* del terrorismo.

In particolare, si sono registrate tre stagioni normative, specchio delle rispettive fasi storiche del fenomeno: a dimostrazione del fatto che il legislatore è incapace di elaborare a monte strumenti duraturi ed unitari di lotta, e va piuttosto predisponendo una strategia di contrasto di tipo emergenziale, prendendo atto in preda alla contingenza del momento delle sue più recenti estrinsecazioni in concreto[12].

[9] Tale rilievo è emerso dallo studio realizzato dallo UNODC, *The use of the Internet for terrorist purposes*, in www.unodc.com.

[10] Sul ruolo dei nuovi mezzi di comunicazione di massa nelle dinamiche del terrorismo internazionale, Flor (2017), p. 320 ss. e Vidino (2014), p. 24 ss. Un affresco dei casi più significativi si può leggere in Dambruso (2018), p. 55 ss.

[11] Per un'analisi più approfondita di tali funzioni, anche in relazione agli interventi legislativi, Fasani (2019), p. 109 ss.

[12] Il risultato è che tutta la legislazione antiterrorismo, nata in una dimensione emergenziale e quindi, per propria natura destinata a durare

Tra tutte, la novella del 2015 rappresenta la sede della più rilevante anticipazione della tutela penale scaturita dalla nuova politica criminale di matrice securitaria[13].

Ne deriva un sistema caratterizzato per la punibilità di condotte molto distanti da una – anche solo – possibile lesione o messa in pericolo del bene giuridico.

Ciò in spregio alle regole generali degli artt. 56 e 115 c.p. che sanciscono l'irrilevanza di atti meramente preparatori o di ideazione, nonché ai principi di rilievo costituzionale di materialità, offensività, legalità *sub specie* determinatezza/prevedibilità e delle funzioni legittime della pena.

L'intera normativa antiterrorismo è costellata da un'anticipazione "estrema": incriminazioni "minuziosamente generiche", spesso solo "simboliche", costruite su base prevalentemente soggettivistica e rispetto alla cui applicazione, legata a esigenze processuali, l'organo giurisdizionale gode di una discrezionalità intollerabile[14].

Vale la pena menzionare alcune delle più rilevanti fattispecie anticipatorie in materia che, nel dare rilevanza a profili meramente comunicativi, possono essere incluse nella categoria dei reati di opinione.

L'art. 270-*quater* c.p. incrimina l'arruolamento (dal 2015, anche nella forma passiva) e la giurisprudenza è arrivata a riconoscere la punibilità finanche del tentativo di tale condotta del tutto indeterminata, anche se solo sul versante attivo[15].

Analogamente, comporta la criminalizzazione di una condotta squisitamente verbale la propaganda di viaggi in territorio estero finalizzati al compimento di atti con finalità di terrorismo, così come descritta dall'art. 270-*quater*.1 c.p.

In questa direzione, si colloca anche il reato di cui all'art. 270-*quinquies* c.p. laddove ammette la punizione delle parole di addestramento o di chi fornisce istruzioni.

Merita, inoltre, un cenno la cospirazione politica mediante accordo che, prevista dall'art. 304 c.p., è potenzialmente idonea a colpire la semplice attività di comunicazione, nella forma dell'accordo diretto a realizzare reati di terrorismo.

Un siffatto andamento normativo comporta una vera e propria "pan-penalizzazione". Essa è ravvisabile nell'incremento asistematico dell'area del penalmente rilevante attraverso l'arricchimento del catalogo codicistico degli illeciti, così come nel continuo innalzamento dei limiti edittali di pena e nella trasformazione dei reati plurisoggettivi da impropri a propri.

Ne è conseguita la previsione di una vera e propria *escalation* terroristica che, in una scala di crescente intensità, punisce l'arruolatore, l'arruolato, l'addestrato, l'autoaddestrato ed infine l'associato.

Da qui deriva il *punctum dolens* rispetto alla libertà di manifestazione del pensiero, giacché si finisce per legittimare l'utilizzo della sanzione penale contro le più remote forme di adesione psicologica alla causa terroristica. Il rischio è quello di punire, etichettandoli quali pericolosi terroristi internazionali, dei – pur odiosi – integralisti religiosi.

Ma vi è di più.

La germinazione del *genus* dei "reati di opinione" nell'ambito della normativa antiterrorismo è dovuta in particolare modo alla rivitalizzazione legislativa che in questo settore hanno ricevuto istigazione e apologia, classiche fattispecie di parola[16].

È significativo rilevare che già prima del 2001 il nostro sistema prevedeva ben tre norme volte a punire la condotta di chi fa apologia o istiga altri a commettere reati in materia di terrorismo.

Si sanciva e si sancisce ancora oggi la punibilità, rispettivamente: di chi fa l'apologia di uno o più delitti ai sensi dell'art. 414, comma 3, c.p.; di chi, pubblicamente, istiga taluno a commettere uno o più reati, per il solo fatto dell'istigazione ai sensi dell'art. 414, comma 1, c.p.; nonché, con specifico riguardo ai soli delitti contro la personalità dello Stato, di chi commette un'istigazione privata, diretta cioè a una o più persone determinate ai sensi dell'art. 302 c.p.[17]

per breve tempo, invece, in realtà, si va stabilizzando. Siamo di fronte ad una "cronicizzazione dello stato d'allerta, una normalizzazione delle misure eccezionali". Cfr. Agamben (2003).

[13] Sul punto: Cavaliere (2015), p. 226 ss. L'Autore riflette sulla violazione dei principi costituzionali di determinatezza, offensività e delle funzioni legittime della pena nella nuova politica criminale antiterrorismo.

[14] Marino (2017), p. 49 ss.

[15] Cass., 9 settembre 2015, n. 40699, *Elezi*, par. 3.1., 17-18, in www.archiviopenale.it. Sull'argomento anche De Marinis (2017).

[16] Fa riferimento a questa tendenza Fronza (2016), p. 1016 ss. Per una analisi generale dell'applicazione giurisprudenziale di tali fattispecie, non solo nel settore terroristico, sia consentito il rinvio a Cirillo (2019), p. 1292 ss.

[17] Il reato di "Istigazione a commettere alcuno dei delitti contro la personalità dello Stato" ex art. 302 c.p. è l'unica fattispecie di istigazione a commettere reati prevista nel nostro ordinamento. Si tratta di un'ipotesi speciale di delitto rispetto alla figura generica di istigazione a

Recentemente, sia il delitto di apologia sia quello di istigazione, nella sua duplice forma, sono stati oggetto di interventi riformatori in chiave repressiva proprio allo scopo di assicurare un più efficace contrasto al terrorismo internazionale.

Nello specifico, le fattispecie in esame sono state arricchite da due circostanze aggravanti.

La prima, inserita con il D.L. n. 144 del 2005, ancora l'aumento di pena della metà se i fatti di istigazione o apologia riguardano delitti di terrorismo o crimini contro l'umanità.

La seconda, introdotta nel recente D.L. n. 7 del 2015, comporta un innalzamento della pena se il fatto è commesso attraverso strumenti informatici o telematici in ragione, come si è visto, della particolare diffusività e conseguente insidiosità di tali mezzi[18].

I due interventi sono stati tacciati di avere carattere essenzialmente simbolico, giacché l'irrigidimento del trattamento sanzionatorio – vanificabile tramite lo schema del bilanciamento *ex* art. 69 c.p. – risulta ispirato a logiche anticipatorie e di rigore sanzionatorio, proprie di un diritto penale d'autore.

Con particolare riferimento alla prima aggravante, vi è da rilevare che i fatti oggetto della stessa sarebbero già stati penalmente rilevanti ai sensi dell'art. 414, comma 1, c.p., che rinvia a una serie aperta di delitti e contravvenzioni, comprendendo senza dubbio anche i reati di terrorismo[19].

Al di là dell'opportunità politico-criminale di tali novelle, dal complesso delle modifiche emerge chiaramente la tendenza descritta. Il legislatore punta sull'arretramento della soglia d'intervento penale, fino a far registrare una sensibile proliferazione della categoria dei reati di opinione: da un lato, mediante la previsione di plurime fattispecie che anticipano notevolmente l'inizio della punibilità intaccando la libertà di parola; dall'altro lato, attraverso la rivalutazione dei tradizionali delitti d'opinione, quali apologia e istigazione.

3. Il formante sovranazionale.

Spinte sempre più considerevoli, nella direzione della criminalizzazione dell'opinione nel settore in esame, provengono anche da parte degli ordinamenti sovranazionali.

Anche l'espansione delle fattispecie di parola condivide, dunque, il dato proprio della maggior parte delle disposizioni italiane finalizzate al contrasto del terrorismo internazionale: quello di trarre origine dalla normativa di matrice internazionale[20].

In questa prospettiva un ruolo di primo piano lo ha svolto l'Unione Europea che, come è noto, fin dal 1999 si è occupata della lotta al fenomeno terroristico: prima, nell'ambito delle politiche del terzo pilastro; oggi, a seguito della comunitarizzazione avvenuta con il Trattato di Lisbona, in base alla competenza penale indiretta *ex* art. 83 TFUE[21].

A questi *inputs* si associano anche le numerose misure adottate in seno al Consiglio d'Europa, al fine di dare attuazione alle indicazioni provenienti dalle Nazioni Unite, quali la Convenzione per la prevenzione del terrorismo del 2005 e il Protocollo Addizionale del 2015[22].

Per quello che interessa in questa sede, è opportuno richiamare la recente Direttiva UE 541/2017 che, oltre a prevedere nuovi obblighi di incriminazione, estende ai nuovi reati l'ambito di applicazione del delitto di istigazione e, inoltre, sollecita gli Stati membri nella punizione della c.d. "pubblica provocazione", anche indiretta, a commettere reati terroristici[23].

Quest'ultima richiesta era già stata anticipata dalla decisione quadro 2008/919/GAI che, nel tentativo di adeguare il sistema normativo alle inedite caratteristiche strutturali di un terrorismo sempre più molecolare, invitava alla criminalizzazione della "*diffusione, o di qualunque altra forma di pubblica divulgazione, di un messaggio terroristico con l'intento di istigare a*

delinquere ex art. 414 c.p. La peculiarità dei beni protetti dal Libro II, Titolo I del codice penale ha giustificato l'estensione della punibilità anche rispetto a condotte non caratterizzate dal requisito della pubblicità. Cfr. Fiandaca e Musco (2012), p. 93 ss.

[18] Parla di un probabile effetto suggestivo dei messaggi istigatori trasmessi mediante strumenti informatici e telematici su una massa generalizzata di persone Leotta (2016), p. 6 ss.

[19] Sul punto, Pelissero (2010), p. 242.

[20] Sul ruolo degli *inputs* internazionali nella normativa italiana di contrasto al terrorismo internazionale: Fasani (2015), p. 929 ss.; Masarone (2013), p. 319 ss.

[21] Sulle competenze dell'Unione Europea nel diritto penale, *ex multis*, v. L. Picotti (2011), p. 207 ss.

[22] Sui riflessi (ante Trattato di Lisbona) delle determinazioni ONU (anche in materia di terrorismo) a livello europeo e interno, cfr. Sciarabba (2006), p. 175 ss.

[23] Il riferimento alla "provocazione indiretta" è nel Titolo 3, articolo 5 della Direttiva UE 541/2017. Quest'ultima Direttiva ha l'obiettivo di sostituire le precedenti decisioni quadro al fine di adeguare nuovamente la normativa all'evoluzione delle minacce terroristiche.

commettere uno dei reati di terrorismo, qualora tale comportamento dia luogo al rischio che possano essere commessi uno o più reati"[24].

Si tenga presente che la stessa definizione era contenuta anche nell'art. 5 della Convenzione del Consiglio d'Europa sulla prevenzione del terrorismo del 2005.

Ribadendo la necessità di introdurre il reato di "pubblica provocazione", la Direttiva del 2017 precisa che lo stesso può realizzarsi con qualsiasi mezzo, sia *online* che *offline,* essendo sufficiente che il comportamento, direttamente o indirettamente, ad esempio mediante l'apologia di atti terroristici, promuova il compimento di reati di terrorismo.

Vengono anche individuati a titolo esemplificativo una serie di atti da incriminare: "l'*esaltazione di attentatori suicidi, l'incoraggiamento ad aderire a jihad violente, l'incitazione diretta a uccidere gli infedeli, la giustificazione del terrorismo o la diffusione di messaggi o immagini di brutali assassini quale mezzo per pubblicizzare la causa dei terroristi o dimostrare il loro potere laddove tale comportamento crea di fatto il rischio che siano commessi atti terroristici a condizione che i messaggi siano diffusi allo scopo di favorire le attività terroristiche, anche qualora la diffusione degli stessi si realizzi per il tramite di Internet*"[25].

In buona sostanza, il legislatore europeo chiede che siano punite, accanto alla classica istigazione diretta, anche forme d'istigazione indiretta, che si limitino cioè ad aumentare il rischio che siano commessi delitti di terrorismo.

Si tratta di una condotta delineata in termini particolarmente generici, che rende indefinita la linea di confine che separa "*freedom of speech*" e apologia di reato terroristico; conseguentemente, rischia di porsi al di là del *discrimen* costituzionale e convenzionale individuato nel rapporto tra esigenza di tutela della collettività e libera manifestazione del pensiero.

Eppure, l'*input* sovranazionale verso l'espansione dei reati di opinione sembra avere un certo seguito. Esemplificativamente, nel nostro ordinamento, tra i tentativi fatti – almeno fino a questo momento – nella direzione richiesta dall'Unione Europea e dal Consiglio d'Europa, va segnalato un disegno di legge presentato alle Camere e non discusso, con il quale si prevedeva l'introduzione dell'art. 270-*octies* c.p., contenente una nuova fattispecie di "istigazione al terrorismo" che avrebbe dovuto punire la pubblica diffusione di messaggi che incitano, anche in maniera indiretta, a commettere atti terroristici[26].

4. Il formante giurisprudenziale.

La tendenza alla riemersione dei reati di opinione nella lotta al fenomeno terroristico si rinviene, oltre che sul versante legislativo (interno ed esterno), anche – anzi, soprattutto – in sede giudiziaria.

Essa si riflette nell'indirizzo ermeneutico favorevole all'estensione applicativa delle fattispecie incriminatrici: si forzano le maglie del tessuto delle – già di per sé onnivore – disposizioni codicistiche fino a rasentarne in modo sensibile la compatibilità con il significato più profondo della democrazia politica, quale la libertà di manifestazione del pensiero[27].

A livello giurisprudenziale, dunque, viene ulteriormente estremizzata quell'anticipazione dell'intervento penale che il legislatore ha cercato di assicurare già a livello di costruzione normativa del catalogo delittuoso.

Tale esasperazione pan-penalistica, che rischia di colpire con la sanzione penale attività di mero proselitismo, si registra lungo due direzioni verso cui l'ermeneutica giudiziaria sembra indirizzarsi.

Da un lato, si assiste ad un'anticipazione della tutela rispetto agli ordinari delitti in tema di terrorismo internazionale, per di più attraverso la definizione del loro rapporto con il tentativo di cui all'art. 56 c.p[28].

[24] Art. 1 della Decisione Quadro 2008/919/GAI. Nello specifico, il nuovo reato era definito all'art. 3, paragrafo 1, lettera a). Si tenga presente che la medesima Decisione integrava l'art. 4, comma 1, della Decisione Quadro 2002/475/GAI che prescriveva la necessità di rendere punibile l'istigazione a commettere reati terroristici, reati riconducibili ad un'organizzazione terroristica e reati connessi ad attività terroristiche.

[25] L'esemplificazione è presente nell'art. 5 della proposta di direttiva 2015/0281, approvata dal Parlamento europeo e dal Consiglio con la risoluzione legislativa del 16 febbraio 2017.

[26] Si fa riferimento al disegno di legge n. 1799, approvato dal Consiglio dei Ministri nella seduta del 20 luglio 2007 e presentato in Parlamento in data 18 settembre 2007 dai Ministri degli Affari Esteri e della Giustizia. Sul punto, Nardi (2017), p. 129 ss.

[27] Sul rapporto tra diritto penale e democrazia all'interno della cultura giuridica occidentale contemporanea caratterizzata da radicali cambiamenti cfr. Merli (2006), p. 8 ss.

[28] Le criticità della tendenza giurisprudenziale a configurare finanche il tentativo delle ipotesi delittuose in materia di terrorismo, già di per sé

Dall'altro lato, si procede ad una rivitalizzazione di quelle fattispecie tipicamente d'opinione (istigatorie e, soprattutto, apologetiche) che, come si è detto, di recente sono state aggiornate in senso repressivo da parte del legislatore.

Concentrandoci su quest'ultimo aspetto, che più specificamente interessa in questa sede, va segnalato che la giurisprudenza, di fronte al drastico incremento degli episodi di esaltazione pubblica della causa terroristica, ha contribuito in maniera rilevante alla (ri)espansione della categoria delittuosa in esame.

Tale rilievo trova conferma, innanzitutto, nella dimensione statistica. La stragrande maggioranza delle pronunce della giurisprudenza, sia di legittimità sia di merito, in tema di istigazione e apologia di delitto riguarda proprio i reati con finalità di terrorismo. Basta una rapida analisi delle banche dati della Suprema Corte di Cassazione per rendersi conto che nell'ultimo biennio non si registra alcuna massima di sentenza rispetto al delitto *ex* art. 414, comma 3, c.p. con oggetto illeciti diversi da quelli attinenti alla materia terroristica.

La straordinaria frequenza applicativa di queste fattispecie di parola ha condotto il potere giudiziario a fare i conti con le delicate questioni – alcune più classiche, altre più inedite – che le medesime sollevano.

Un dato è comune ai diversi arresti. La quasi totalità degli stessi, inserendosi nella tradizionale e complicata individuazione dei criteri discretivi tra legittima manifestazione del pensiero e condotta penalmente illecita, aderisce, almeno in linea di astratta dichiarazione di principio, alla posizione di cui, da tempo, è fautrice la Consulta.

Come è noto, a partire dagli anni sessanta la Corte costituzionale, con diverse sentenze interpretative di rigetto, ha sempre salvato i reati di opinione dal conflitto con l'art. 21 della Costituzione[29], pur minacciato da autorevole dottrina[30].

La strada suggerita trova la sua "pietra miliare" nella sentenza n. 65 del 1970, proprio in riferimento all'apologia: interpretare le principali fattispecie in esame in chiave costituzionale facendo leva sul principio di offensività nella sua accezione in concreto[31].

Ne deriva una manipolazione della tipicità di tali ipotesi delittuose: corroborate dal requisito oggettivo dell'idoneità, sono trasformate da reati legislativamente configurati a pericolo presunto in reati a pericolo concreto (c.d. "implicito")[32].

È chiaro che, con una siffatta costruzione, la selezione del tipo di condotta rilevante spetterà all'interprete con conseguenze, come si vedrà, problematiche.

Per non collidere con la Costituzione, l'apologia punibile va letta, con una sorta di *abolitio criminis* dell'originaria fattispecie, alla stregua di una "istigazione indiretta": non sarà la mera esaltazione di un reato ma quella che sia "concretamente idonea a provocare la commissione di delitti"[33]. E l'argomento vale per qualsiasi altra incriminazione d'opinione.

A conclusioni analoghe è giunta, altresì, la Corte Europea dei diritti dell'uomo, chiamata in diverse occasioni a valutare la compatibilità dei reati di opinione, ancora oggi presenti in larga parte degli Stati Europei, con la libertà di espressione riconosciuta dall'art. 10 CEDU[34].

4.1. *Il depotenziamento giudiziale del pericolo concreto nel "mondo virtuale".*

Come si è anticipato, anche le più recenti sentenze in materia di istigazione e apologia con cui si tenta di far fronte al rischio terroristico seguono, nelle premesse, questo assunto.

È frequente leggere che al fine di integrare i delitti in questione non basta "l'esternazione di un giudizio positivo su un episodio criminoso, per quanto odioso e riprovevole possa ap-

a forte connotazione anticipata, sono ben evidenziate da Marino (2017), p. 47 ss.

[29] V. Corte Cost., sentenze nn. 87/1966, 84/1969, 16/1973, 65/1970, 108/1974.

[30] Sui profili di incostituzionalità dei reati di opinione cfr. Fiore (1972), *passim*.

[31] Corte Cost., sentenza n. 65 del 1970 con nota di Bognetti (1971), p. 18 ss.

[32] Il duplice ruolo, in astratto e in concreto, del principio di offensività è, da qualche tempo, riconosciuto e ribadito, sulle spinte della dottrina, anche dalla Corte Costituzionale. In questi termini: Corte cost. n. 265/2005. In dottrina, Fiandaca e Musco (2009), p. 152 ss.

[33] Cass., Sez. I, 17 novembre 1997, n. 11578, Gizzo; Cass., Sez. I, 5 maggio1999, n. 8779, Oste. Questa impostazione sembra essere condivisa anche dalle pronunce più recenti della giurisprudenza di legittimità: tra tutte, Cass., Sez. I, 6 ottobre 2015, n. 47489, *Halili*.

[34] Nicosia (2006), p. 209 ss. A giudizio della Corte le condotte devono presentare un carattere di pericolosità per interessi pubblici significativi, così da essere direttamente o indirettamente prodromiche o favorevoli alla realizzazione di attività criminali. Da ultimo, Corte Edu, 9 maggio 2018, *Stomakhin c. Russia*. Interessante anche la prospettiva di Corte Edu, 7 marzo 2019, *Sallusti c. Italia*, dove, anche se con riguardo alla fattispecie di diffamazione, si sottolinea la sproporzione della pena detentiva nei casi in cui è interessata la libertà di espressione.

parire alla generalità delle persone dotate di sensibilità umana". Piuttosto, si sostiene che il comportamento dell'agente debba essere "per il suo contenuto intrinseco, per la condizione personale dell'autore e per le circostanze di fatto in cui si esplica" idoneo a determinare il "rischio, non teorico ma effettivo, della consumazione di altri reati e, precipuamente, di reati lesivi di interessi omologhi a quelli offesi dal crimine esaltato"[35].

Evidentemente, attraverso una valutazione siffatta dovrebbe essere scongiurata la punizione della pura e semplice manifestazione del pensiero.

Sennonché, approfondendo le motivazioni e le conclusioni delle varie pronunce, emerge, ancora una volta, un dato in comune. La particolarità è che esso si palesa come diametralmente opposto rispetto alle appena esaminate dichiarazioni di principio.

Dall'analisi delle sentenze l'impressione è che, a dispetto delle premesse costituzionalmente orientate, quello che viene formalmente chiamato pericolo concreto assomigli molto nella sostanza al pericolo presunto.

Nello specifico, il depotenziamento dei profili offensivi trova, nell'ambito della prassi applicativa, almeno tre indici rivelatori.

Innanzitutto, il pericolo è solo raramente rapportato alla commissione di un reato con finalità di terrorismo. È, invece, spesso segnato dalla condizione personale del soggetto agente; e frequentemente accade che questa è misurata dal legame con altri soggetti già indiziati di delitti terroristici[36].

Si approda, dunque, ad applicazioni giudiziali che tengono conto in massima parte del *background* personale dell'imputato, tralasciando la reale esposizione a pericolo dei beni giuridici dell'ordine pubblico e della sicurezza collettiva[37].

La circostanza che nelle valutazioni sul pericolo da parte dei giudici – sia di merito che di legittimità – sia assorbente il dato della biografia personale del soggetto agente e, nello specifico, i contatti con individui anche solo indagati per delitti terroristici dimostra la natura soggettivamente pregnante delle disposizioni d'opinione, almeno con riferimento alla materia dell'antiterrorismo[38].

Così, il diritto penale del fatto rischia di diventare diritto penale d'autore, persino in sede di applicazione giudiziaria.

Con tutta evidenza, già questo prima dato, nella misura in cui rileva i caratteri propri di fattispecie giudizialmente costruite su base soggettivistica, sarebbe sufficiente a provare la svalutazione dell'elemento del pericolo concreto nelle dinamiche della prassi ermeneutica.

Vi è però un secondo elemento da tenere in considerazione. In questa materia, l'arretramento della tutela penale ai margini della libertà di manifestazione del pensiero emerge con nettezza poiché come delitto oggetto di apologia o istigazione è frequentemente contestata la partecipazione ad associazione con finalità di terrorismo.

L'innesto giudiziale tra i due reati, sebbene sia considerato dalla giurisprudenza di legittimità "dato ermeneutico incontroverso", sarebbe bisognoso di maggiori approfondimenti[39].

Se, come fin qui si è dimostrato, l'istigazione e l'apologia sono illeciti a consumazione anticipata, non è da meno il delitto previsto dall'art. 270-*bis* c.p. Anzi, l'associazione con finalità di terrorismo è costantemente considerata dalla giurisprudenza un reato di pericolo presunto, per il quale è sufficiente la presenza di una struttura organizzativa anche rudimentale, con grado di effettività tale da rendere possibile l'attuazione del programma criminoso, senza che

[35] In termini sostanzialmente analoghi: Cass., Sez. I, 6 ottobre 2015, n. 47489, *Halili*; Cass., Sez. I, 28 giugno 2016 n. 31249; Cass., Sez. I, 3 novembre 2016, n. 46175, *El Hanaoui* (in materia di istigazione); Cass., Sez. I, 15 maggio 2017 n. 24103, *Dibrani*; Cass., Sez. V, 25 settembre 2017, n. 55418. La prima con nota di Zirulia (2015) e Rossi (2016), p. 2470 ss.

[36] A titolo esemplificativo, si veda Cass., Sez. V, 25 settembre 2017, n. 55418 con nota di Cirillo (2018). La Corte censura la pronuncia del Tribunale del Riesame che aveva annullato l'ordinanza di custodia cautelare emessa nei confronti di un soggetto ritenuto gravemente indiziato del reato di cui all'art. 414 comma 4 c.p. per aver pubblicamente, attraverso la diffusione sulla rete *Internet*, fatto apologia dello Stato Islamico, proprio perché "non aveva tenuto conto dei contatti dell'indagato con altri soggetti già indagati per terrorismo islamico".

[37] In senso critico sulla capacità selettiva di beni siffatti, anche nel contrasto al fenomeno terroristico: Cavaliere (2009), p. 43 ss.

[38] Si badi: tale tendenza giudiziale non è esclusiva dei soli reati di opinione in senso stretto (apologia e istigazione) utilizzati in funzione antiterrorismo, ma si estende alla maggior parte dei delitti previsti in materia e caratterizzati da una c.d. "anticipazione estrema". Sul versante giurisprudenziale è significativa la sentenza, in materia di tentativo di arruolamento *ex* art. 270-*quater* c.p., Cass., 9 settembre 2015, n. 40699, *Elezi*. In dottrina spunti critici in Pellissero (2016), *passim*.

[39] Secondo la giurisprudenza di legittimità è incontroverso che il pericolo concreto possa concernere "non solo la commissione di specifici atti di terrorismo, ma anche, la partecipazione di taluno ad un'associazione di questo tipo". Cfr. Cass., Sez. I, 9 ottobre 2018, n. 51654 e Cass., Sez. V, 25 settembre 2017, n. 55418. Sulle ombre di questa impostazione che rischierebbe di incentivare fenomeni di criminalizzazione ad ampio spettro, Mazzanti (2017), p. 34 (in riferimento a Cass., Sez. I, 6 ottobre 2015, n. 47489, *Halili*). Inoltre, che le consorterie di ispirazione *jihadista* operanti su scala internazionale abbiano natura di organizzazioni terroristiche è orientamento consolidato: cfr. Cass., Sez. V, 8 ottobre 2015, n. 2651, *Nasar Osama*, Rv. 265925; Cass., Sez. V, 4 luglio 2016, n. 48001, *Hosini*, Rv. 268164.

sia neppure richiesto l'inizio dell'esecuzione dell'attività programmata[40].

Pertanto, innestare tra loro due delitti costruiti sul "pericolo", e per di più oggetto di interpretazioni estensive da parte della giurisprudenza, determina una duplice anticipazione della tutela, di dubbia compatibilità con i principi costituzionali. Addirittura, l'anticipazione sarebbe triplice se si tiene conto della sede cautelare in cui spesso si trova a pronunciare la Corte, per cui il pericolo da accertare è il requisito necessario per l'applicazione della misura.

Ma vi è di più. La tendenza al depotenziamento della dimensione offensiva dei reati di opinione non è soltanto indicata dal ruolo assorbente che svolge, nelle valutazioni giudiziali, la condizione personale dell'autore e dalla frequente combinazione di reati di pericolo.

Vi è, infatti, una terza spia – forse più sottile, ma non meno rilevante – del depotenziamento offensivo.

I giudici concentrano l'accertamento del pericolo concreto sulle modalità esplicative delle condotte apologetiche e istigatorie. Nello specifico, se queste, come spesso avviene, sono realizzate mediante l'utilizzo di strumenti telematici non solo vengono considerate idonee ad integrare la natura pubblica richiesta *ex* art. 414 c.p. per la configurazione dei relativi delitti; ma sono ritenute anche, e automaticamente, concretamente pericolose[41].

Il presente rilievo conduce a due considerazioni.

Da un lato, senza dubbio, le Corti mostrano di non sottovalutare il ruolo fondamentale svolto dai moderni dispositivi di comunicazione di massa nel diffondere il radicalismo islamico. Sul punto, è costantemente ripreso l'orientamento consolidato che ai fini della natura pubblica della condotta, definita dall'art. 266, comma 4 c.p., richiede una "potenzialità diffusiva indefinita" della comunicazione (equiparabile alla stampa)[42]. Di conseguenza, si ritiene che la medesima sia riscontrabile anche nelle ipotesi di diffusione di messaggi apologetici/istigatori sui *social network*, considerabili alla stregua di "siti *Internet* privi di vincolo di accesso"[43].

D'altro lato, il ragionamento della giurisprudenza – pur corretto in relazione a questo primo aspetto – rileva la sua criticità quando l'accertamento dell'elemento della pubblicità della condotta assorbe quello del pericolo concreto: in altri termini, per i giudici se una comunicazione è pubblica sarà anche concretamente pericolosa, senza bisogno di ulteriori approfondimenti[44].

Si finisce, cioè, per considerare insito al concetto espresso di "pubblicamente" una presunzione, quasi assoluta e difficilmente vincibile, di pericolosità.

Eppure, il fatto stesso che una condotta sia esternata in pubblico, non significa necessariamente che determini un concreto pericolo di istigazione[45].

Quest'ultimo rappresenta una garanzia in più rispetto al mero carattere pubblico della condotta. Pertanto, la giurisprudenza dovrebbe punire, al netto della loro pubblicità, solo quelle comunicazioni capaci di ledere concretamente i beni protetti, anche solo nella forma della messa in pericolo.

Tra l'altro, che una condotta debba essere pubblica ai fini della sua rilevanza penale, può forse considerarsi un'esigenza "anacronistica" da quando *Internet* e i nuovi mezzi di comunica-

[40] Fasani (2016), pp. 237 ss., 393 ss., 418 ss. L'Autore parla di una giurisprudenza plasmante che, pur di giungere a giudizi di responsabilità, ha modellato il reato associativo sulla "sagoma dei nuovi gruppi estremisti": infrangendo il paradigma ermeneutico garantista tradizionalmente elaborato in materia di reati associativi, gli elementi cardine dell'esistenza del reato in esame (associazione, partecipazione e dolo) sono stati adattati "alle forme del nemico". Esempi di questa giurisprudenza si rinvengono in: Cass., Sez. VI, 8 maggio 2009, n. 25863; Cass., Sez. II, 25 maggio 2006, n. 24994. Sulle più recenti concezioni estensive in tema di partecipazione ad associazione terroristica, Giordano (2019), pp. 274 ss.

[41] Da ultimo, Cass. Sez. I, 8 febbraio 2018, n. 20198; Cass., Sez. I, 15 maggio 2017, n. 24103, *Dibrani*: "ai fini della configurabilità della fattispecie di cui all'art. 414 c.p. non rileva la tipologia dei reati in relazione ai quali si esplica l'attività comunicativa, ma le modalità con cui la comunicazione viene esternata".

[42] L'orientamento è ormai granitico nella giurisprudenza di legittimità. Cfr. Corte di Cassazione, Sez. I, 23 aprile 2012, n. 25833, Testi; Sez. I, 5 giugno 2001, n. 26907, Vencato.

[43] Su questo aspetto cfr. Cass., Sez. I, 6 ottobre 2015, n. 47489 *Halili* e Sez. I, 15 maggio 2017, n. 24103, *Dibrani*. In quest'ultima sentenza la Corte ha escluso la sussistenza del reato relativamente a comunicazioni telematiche (anche di un *social network*) meramente private e interpersonali; lo ha invece ritenuto configurato relativamente a videoregistrazioni di contenuto apologetico dell'*Isis* e del terrorismo di matrice islamica diffuse tramite il *social network Facebook* in quanto "tale modalità ha una potenzialità diffusiva indefinita".

[44] Cfr. Cass., Sez. V, 25 settembre 2017, n. 55418 dove si riconosce valore assorbente, al fine di configurare il delitto apologetico, proprio alla "funzione propalatrice di condizionamento delle coscienze" svolta in tale delicata materia dal *social network Facebook*.

[45] Giova segnalare che il tema è emerso, con tutte le sue implicazioni, anche nel travagliato *iter* parlamentare che ha condotto alla legge n. 115 del 2016 con cui si è introdotta la c.d. "aggravante del negazionismo". L'accesa discussione, durante i lavori preparatori, sull'alternativa tra un requisito più esplicito di istigazione e quello della "pubblicità" della condotta si è tradotta nell'emendamento 1.401 (c.d. D'Ascola) con cui si è ritenuto maggiormente garantistico il "concreto pericolo di diffusione". In quella sede non è mancato chi, ritenendo che si tratti di un fenomeno che non tutti ritengono di dover contrastare con il diritto penale, l'utilizzo di una ripetizione avrebbe espresso un maggiore richiamo ai principi costituzionali. Sull'argomento, *ex multis*, Scotto Rosato (2016), p. 292 ss.; Pulitanò (2015), p. 325 ss.

zione hanno definitivamente demolito il confine tra pubblico e privato[46].

Ebbene, l'assorbimento del giudizio di pericolosità delle parole nella constatazione della loro natura pubblica è nient'altro che la naturale conseguenza del ruolo che i nuovi strumenti di comunicazione svolgono nelle dinamiche jihadiste.

I vantaggi che ottengono gli estremisti dall'uso massiccio dei canali informatici trovano il loro contraltare nei problemi di non poco momento relativi all'accertamento della tipicità dei reati in questione.

Si è visto che le indicazioni costituzionali e convenzionali ne subordinano la legittimità all'accertamento dell'idoneità offensiva, da vagliare alla luce del concreto contesto di svolgimento delle condotte verbali.

Si tratta di un giudizio complesso già quando ha ad oggetto comunicazioni espresse nel mondo reale.

Laddove, poi, si devono ricercare gli effetti delle parole pronunciate in contesti virtuali l'indagine diventa inevitabilmente più confusa, se non del tutto velleitaria. Deve, infatti, fare i conti con un contorno fattuale sfuggente, globale e aperto, senza precisi e sicuri indici per valutare l'effettività della minaccia jihadista.

Nello specifico, vi sono casi in cui la rete *web* costituisce semplice proiezione dell'ambiente reale (si pensi, ad esempio, alle *chat* o ai *forum*), per cui l'accertamento della concretezza del pericolo terrorista, seppure affievolito, potrebbe essere compiuto secondo gli schemi tradizionali.

Nella maggioranza delle ipotesi della casistica giurisprudenziali, in cui, invece, gli strumenti di comunicazione rappresentano veicoli *erga omnes* per i messaggi estremisti, il giudizio di potenziale idoneità risulta del tutto slabbrato. Così che, come dimostrano le recenti pronunce in materia, l'unica forma di concretizzazione del pericolo vagliata dai giudici è relativa al contenuto oggettivamente apologetico e pubblico delle parole: basterebbe ciò per rendere probabile l'adesione all'islamismo militante[47].

Le considerazioni fin qui svolte dimostrano la scarsa rilevanza attribuita, nello *standard* giudiziario, al pericolo concreto delle fattispecie istigatorie e apologetiche antiterrorismo: attenzione assorbente al *background* personale dell'agente e al canale informatico utilizzato, nonché innesto tra reati a consumazione anticipata ne sono efficaci dimostrazione.

L'inevitabile conseguenza è la riemersione, in questo settore, di reati di opinione svincolati da ogni tipo di valutazione attinente al profilo dell'offensività e di dubbia compatibilità con la libertà di manifestazione del pensiero.

In realtà, il depotenziamento della carica lesiva nei reati in esame non deve meravigliare più di tanto.

In tutti i delitti di opinione la prova del passaggio dalle parole al pericolo dei fatti è di complessa individuazione a causa di una pluralità di fattori.

Le difficoltà, che si amplificano a dismisura per le comunicazioni diffuse nel mondo virtuale, sono dovute alla mancanza di plausibili canoni di verificabilità che si registrano sul significato dell'idoneità[48]; nonché, alla circostanza per cui l'oggetto dell'analisi non è un singolo fenomeno naturalistico, ma l'intera realtà socio-politica, facendo approdare sul piano della causalità psicologica.

Ancora, le condotte istigatorie o apologetiche si caratterizzano per un'intrinseca distanza dai fatti, come anche per l'esistenza di una sproporzione di scala tra la "micro-condotta" con cui si esprime il pensiero ed il "macro-evento" di esercizio della violenza che si dovrebbe cagionare[49]; e lo iato è ancora più profondo nel caso dei delitti di terrorismo realizzati tramite il *web*.

La rivitalizzazione dei reati di opinione in questo settore fa (ri)emergere il principale limite della lettura costituzionalmente orientata che di queste fattispecie ha offerto la Consulta. Poiché la selezione delle condotte punibili viene demandata alla pura discrezionalità dell'interprete, senza alcun criterio direttivo controllabile, nulla assicura che il pericolo concreto sia davvero oggetto di indagine e non solo di un'apodittica adesione nominalistica[50].

Come si è visto, le nuove tecnologie usate dai moderni terroristi, rendendo ancor più criti-

[46] Sul confine tra pubblico e privato nella società di oggi, cfr. Rodotà (2013), p. 118 ss.
[47] Fasani (2019), p. 127 ss.
[48] Cfr. Cerase (1993), p. 1715-1720 che distingue tra immediata attitudine e mera possibilità che simili reati siano commessi. Anche la giurisprudenza di legittimità ha fatto ricorso a criteri di volta in volta diversi e scarsamente selettivi. Sul tema si rinvia a Nardi (2016), p. 1128 ss.
[49] Cfr. Pelissero (2015), p. 42.
[50] Riflettono in termini critici sulla selettività del pericolo concreto (implicito) nei reati di opinione, *ex multis*, Pelissero (2015), p. 39, 42.; Viganò (2007), p. 125; Visconti (2008), p. 115.

co il vaglio di pericolosità, contribuiscono ad attualizzare tali riflessioni.

D'altro lato, è innegabile che un rigoroso accertamento del pericolo concreto condannerebbe nella sostanza queste figure ad una totale inutilità: è estremamente inverosimile che un'isolata condotta di apologia, in condizioni di normalità della vita civile dello Stato, possa addirittura comportare pericolo per la sicurezza dello Stato o per la sua tenuta democratica.

5. Profili critici e di compatibilità costituzionale: verso il diritto penale del nemico?

Il quadro appena passato in rassegna, che vede l'intervento di tutti gli attori della sistematica penalistica, dimostra la riemersione nella materia antiterrorismo di reati di opinione puri, in cui è assente ogni valutazione di offensività sulle comunicazioni.

Tale considerazione si riflette plasticamente quando, come si è detto, si punisce per apologia di associazione a fini terroristici chi ha postato sul *social network facebook*, tramite la sola opzione *like,* registrazioni e video relativi all'*Isis*[51].

Il rischio, già paventato, è imbrigliare la libertà di manifestazione del pensiero, pur di far fronte alle nuove e insidiose forme di incitamento e propaganda terroristiche *online*.

In questo peculiare settore l'esatta individuazione della soglia dell' – ineludibile – intervento penale e del confine con la predetta libertà è oltremodo complicata[52].

Al cospetto della nuova vita dei reati di opinione, la questione fondamentale è proprio quella del bilanciamento tra libertà compresse – non solo quella personale, sacrificata da qualsivoglia disposizione incriminatrice, ma soprattutto quella di espressione – e ragioni per le quali le si comprime[53].

Non può sfuggire che la libertà di manifestazione del pensiero ha un valenza costitutiva del nostro ordinamento; in buona sostanza, è ciò che permette di qualificarlo non solo come liberale ma anche personalistico, democratico, laico, pluralista e fondato sull'eguaglianza.

Tutelata nel nostro sistema costituzionale in quanto tale, e non soltanto in quanto "utile alla collettività", tale libertà delinea un modello di democrazia aperta; di conseguenza, segna la sua essenza proprio nel carattere antagonista, conflittuale, pluralista: sarebbe del tutto superflua una libertà dei pensieri innocui e conformi a Costituzione[54].

Anche la Corte europea dei diritti dell'uomo si colloca sulla stessa scia nell'applicazione degli artt. 10 e 11 CEDU[55].

Nonostante tale rilevanza, tradizionalmente, si ritiene che la libertà di manifestazione del pensiero possa essere sottoposta a restringimenti a tutela di interessi ritenuti, all'esito di bilanciamenti, prevalenti[56].

Oltre al limite del buon costume, l'unico normativamente previsto, le altre limitazioni a tale "pietra angolare del sistema democratico" devono essere valutate con molta cautela in coerenza con il criterio di ragionevolezza.

Quanto all'istigazione e all'apologia, per lungo tempo si è ritenuto che la loro legittimità sia garantita dalla protezione dell'ordine pubblico, inteso nella sua accezione materiale costituzionale[57].

Sennonché, da un lato l'inafferrabilità empirica di un concetto di tal fatta, dall'altro le difficoltà connesse all'accertamento del pericolo concreto, anche alla luce dei nuovi strumenti digitali, fanno sì che il principio di offensività sia rispettato solo nella forma, ma eluso nella

[51] A titolo esemplificativo, Cass., Sez. V, 25 settembre 2017, n. 55418.
[52] Sul rapporto tra libertà di espressione e reati di opinione, tra i molti, Spena (2007), p. 697 ss.
[53] Pelissero (2015), p. 37 ss. individua nel bilanciamento degli interessi la caratteristica che accomuna la composita categoria dei reati di opinione. A parare dell'Autore, la stessa va declinata in relazione agli ambiti specifici nei quali si esercita il controllo penale sulla manifestazione del pensiero.
[54] Esposito (1958), p. 10 ss. E' significativa Corte cost., sent. n. 11/1968, che definisce la libertà di manifestazione del pensiero "pietra angolare della democrazia".
[55] Corte europea dir. uomo, 23 settembre 1998, ric. n. 24662/94, *Lehideux et Isorni c. Francia*, dove si legge che tale libertà "*vale non solo per le informazioni o idee accolte con favore o considerate inoffensive o indifferenti ma anche per quelle che offendono, indignano o turbano lo Stato o una qualsiasi parte della popolazione. Così vogliono il pluralismo, la tolleranza e lo spirito di apertura, senza i quali non vi è società democratica*".
[56] Così, Corte. Cost., sent. n. 87/1966. In senso analogo, Corte cost., sentenze nn.19/62;100/1966; 199/1972; 15, 16 e 133 del 1973; 20/1974. Sul versante sovranazionale per un efficace quadro di sintesi sulla questione sia consentito il rinvio a Fronza (2006), p. 31 ss.
[57] Fiore (1980), p. 1084 ss.

sostanza[58].

Pertanto, dinanzi all'espansione dei reati di opinione antiterrorismo i referenti della tutela dovrebbero fare a meno della sicurezza collettiva ed essere individuati, almeno a livello ermeneutico, nei beni individuali direttamente intaccati dagli atti di violenza, quali la vita, la libertà personale e l'incolumità fisica[59]: così da ricondurre le fattispecie *de qua* in linea con le garanzie costituzionali.

Tuttavia, anche siffatti interessi individuali potrebbero prestare il fianco a critiche giacché, nella misura in cui sono svincolati dall'accertamento del pericolo concreto, rischiano di venire in rilievo in una dimensione astratta, caratterizzata da una scarsa verificabilità empirica e da possibili manipolazioni giudiziarie[60].

Si tratta, in buona sostanza, di ciò che già si registra nella prassi ermeneutica, dove – lo si è detto – l'idoneità offensiva rispetto al bene individuale tutelato è sensibilmente affievolita, a favore di una (iper)protezione della sicurezza collettiva.

In questo contesto, dominato dalla minaccia terroristica, non è solo il *law in books* ma anche – e forse soprattutto – il *law in action* a farsi portatore delle istanze general-preventive e securitarie. E la giurisprudenza incontra buon gioco lungo questa direzione, poiché l'applicazione pratica delle fattispecie apologetiche e istigatorie, prive di precisi e selettivi criteri direttivi controllabili, si presta a facili condizionamenti da parte del contesto politico e sociale di riferimento.

Così, la rivitalizzazione del *genus* nel settore dell'antiterrorismo finisce per diventare cartina di tornasole delle metamorfosi e delle trasformazioni che sta vivendo il diritto penale dei nostri giorni.

Da un lato, si assiste ad un suo uso strumentale in chiave preventivo-repressiva. Dall'altro lato, si arriva ad un'esasperata flessibilizzazione dei principi fondamentali: quello cardine, per una democrazia politica, della libertà di manifestazione del pensiero; nonché, quelli tipicamente penalistici di sufficiente determinatezza/prevedibilità, offensività e proporzionalità.

La conseguenza è tradire, anche a livello giudiziale, il diritto penale costituzionalmente orientato – *magna charta libertatum* del reo – per accostarsi alla prospettiva illiberale del diritto penale del "nemico": il terrorista non è solo un criminale ma diventa un vero e proprio *enemy* da combattere con ogni mezzo necessario e utile, anche a costo di comprimerne i diritti fondamentali[61].

A ben vedere, un tale paradigma bellicista non rispecchia – almeno per il momento – la disciplina italiana di contrasto al terrorismo. Com'è stato autorevolmente rilevato, il nostro ordinamento sembra, piuttosto, orientarsi verso un "diritto penale al limite"; in cui, cioè, è sempre alto il rischio che la ragionevolezza delle scelte politico-criminali si traduca, in nome della ragion di stato, in forme illegittime di violazione di quelle garanzie su cui dovrebbe fondarsi il sistema penale costituzionale[62].

Nessuno mette in discussione che nella lotta al terrorismo un ruolo di primo piano debba essere svolto dalla repressione penale. Neppure vi è dubbio circa l'opportunità di anticipare la soglia d'intervento dello strumento criminale, proprio per il carattere nevralgico che assume il pensiero islamico radicale rispetto al fenomeno terroristico in sé. Altrimenti, si rischierebbero di legittimare forme paradossali di abuso del diritto[63].

In questo contesto, la discussione non attiene all'*an* della criminalizzazione di fattispe-

[58] Dubita dell'efficacia selettiva dell'ordine pubblico, *alias* sicurezza collettiva, Cavaliere (2009), p. 43 ss.

[59] Pelissero (2015) p. 40.

[60] Per la ricostruzione di tale impostazione v. Visconti (2008), p. 140 ss. In proposito, è interessante notare il riflesso dell'indirizzo in parola rispetto a quei reati (di opinione) posti già *ex lege* a protezione di beni personali (come l'onore). La tendenza recente, in questa materia, va verso la depenalizzazione in favore di modelli di tutela privatizzati. È il caso, da ultimo, dell'art. 594 (ingiuria) abrogato dal d.lgs. n. 7 del 2016. Spunti in tal senso, con riferimento ad un'auspicata revisione del reato di diffamazione in Gullo (2013), *passim*.

[61] La tesi di una differenziazione del diritto penale, attraverso l'istituzione di un "diritto penale del nemico" accanto al "diritto penale del cittadino", è stata avanzata da G. Jakobs nel 1985 (cfr. la ricostruzione in Jakobs (2007), p. 5 ss.). Il modello delineato dall'Autore mira a neutralizzare la pericolosità individuale di quei soggetti dai quali non ci si può attendere l'osservanza delle regole fondamentali della convivenza civile e si caratterizza per l'arretramento accentuato della tutela penale ad atti preparatori, per gli altissimi livelli sanzionatori e per la riduzione delle garanzie difensive. Nella dottrina italiana, in senso fortemente critico, *ex multis*, Palazzo (2006), p. 676 ss.; Ferrajoli. (2006). Quest'ultimo, in proposito, parla di "una contraddizione in termini, che rappresenta, di fatto, la negazione del diritto penale, la dissoluzione del suo ruolo e della sua intima essenza".

[62] Pelissero (2016), p. 99 ss. Sull'individuazione, in nome della sicurezza collettiva, di un limite tollerabile ai diritti fondamentali, in specie al diritto di manifestazione del pensiero Donini (2007), p. 55 ss.; Bartoli (2008).

[63] In Nardi (2017), p. 74 si legge: "*le stesse garanzie finirebbero per diventare lo strumento utilizzato dai terroristi per conseguire i propri obiettivi e violare altri diritti fondamentali*".

cie tipicamente d'opinione; piuttosto al *quomodo* dell'incriminazione. Deve rimanere saldo un nucleo essenziale di principi rispetto ai quali non è consentito arretrare né in via di astratta previsione legislativa, né tantomeno sul piano dell'ermeneutica giudiziale[64].

Ebbene, come si è avuto modo di esaminare, il sistema dei reati di opinione previsto nel settore dell'antiterrorismo risulta di dubbia compatibilità con diversi capisaldi riconosciuti come fondamentali dalla nostra Costituzione e significativamente valorizzati nella prospettiva sovranazionale.

In primo luogo, le condotte delle fattispecie, descritte in termini fumosi e particolarmente generici, non riescono ad assolvere alla funzione di limite alle virtualità espansive dell'incisivo sistema di contrasto ad un terrorismo islamista che trova nel mondo virtuale il suo terreno di riferimento.

Di conseguenza, le critiche si registrano rispetto al principio di legalità *sub specie* determinatezza. Tale corollario, recentemente riletto a livello convenzionale e costituzionale nell'inedita dimensione qualitativa della prevedibilità da parte del singolo dell'assoggettamento a pena[65], non sembra essere rispettato, stante la difficoltà oggettiva di individuare la condotta tipica offensiva dell'interesse protetto e di descriverla con sufficiente chiarezza.

Inoltre, le disposizioni incriminatrici *de qua* sono particolarmente problematiche in riferimento al principio di offensività, nella misura in cui l'accertamento del pericolo concreto di condotte verbali, per di più diffuse tramite la rete *Internet*, è svincolato da criteri controllabili a priori e risulta sensibilmente influenzabile dal contesto socio-politico di riferimento.

Nello specifico, l'offensività potrebbe venire in gioco declinata sul versante della proporzionalità della pena. Il rischio di incriminare condotte lontane da un'offesa, ancorché nella forma del pericolo, del bene giuridico protetto è quello di far apparire facilmente sproporzionato il ricorso alla pena stessa, soprattutto laddove vi sia una scarsa probabilità che il comportamento vietato si traduca in lesione effettiva[66].

In questi casi, è del tutto lecito dubitare dell'efficacia rieducativa di una tale sanzione criminale. Anzi, punire il singolo facendone un mero strumento per finalità di prevenzione generale (negativa) rischia di risultare criminogeno: di indurre, cioè, a processi di radicalizzazione, opposti a quelli sperati[67].

6. Rilievi conclusivi.

Rispetto alle criticità che solleva il quadro dei reati di opinione, previsti nel contrasto al terrorismo internazionale e attualmente veicolati dai *new media*, sarebbe auspicabile un intervento della Consulta, volto a riallineare il sistema ai capisaldi costituzionali e convenzionali[68].

Come si anticipava, in questa prospettiva, ancor più che il principio di sufficiente determinatezza/prevedibilità, potrebbe avere buon gioco il corollario dell'offensività, letto nella dimensione delle proporzionalità del ricorso alla pena, recentemente valorizzata sia a livello costituzionale che sovranazionale[69].

Anche il legislatore potrebbe fare la sua parte.

A ben vedere, il depotenziamento a livello giudiziario del pericolo concreto dell'apologia è l'inevitabile conseguenza della sovrapposizione normativa che presenta il nostro ordinamento;

[64] Niente di più di quanto Enrico Pessina, oltre centocinquanta anni fa, suggeriva ai giuristi in relazione al *genus* dei reati politici: assicurare la massima salvaguardia dei principi garantistici individuali. Per un'efficace ricostruzione del pensiero giuridico e politico dell'Autore, Maiello (2012), p. 406 ss.

[65] Corte Edu, Grande Camera, sent. 23 febbraio 2017, de Tommaso c. Italia. Per le ricadute di tale arresto nel nostro ordinamento, cfr. Cass., Sez. Un. Pen., 27 aprile 2017 (sent.), n. 40076 e Corte cost., nn. 24 e 25 del 2019. Con riguardo al diritto penale in senso si stretto si veda anche Corte cost., n. 115 del 2018.

[66] Pelissero (2000), p. 128 ss.

[67] Per una riflessione di questo tipo rispetto al tema della "criminalizzazione del dissenso", sia pure non con specifico riguardo al settore dell'antiterrorismo, Forti (2016), p. 1034 ss.

[68] Nella direzione diametralmente opposta si è di recente mosso il Conseil Constitutionnel francese (Décision del 18 maggio 2018 n. 706), fondando la legittimità costituzionale dell'apologia di terrorismo sulla necessità di garantire la prevenzione dei gravi fatti di terrorismo internazionale.

[69] Inaugura un approccio radicalmente nuovo nella valutazione delle proporzionalità della pena per specifici reati, abbandonando il tradizionale requisito del *tertium comparationis*, Corte cost., 10 novembre 2016, n. 236 con nota di Viganò (2017). Sulla stessa scia, Corte cost. n. 222 del 2018 e n. 40 del 2019. Nella prospettiva sovranazionale, valorizza il canone della (s)proporzione della pena (detentiva) quando viene in gioco la libertà di manifestazione di pensiero la già richiamata Corte Edu, 7 marzo 2019, *Sallusti c. Italia* (in riferimento ad un'ipotesi di diffamazione).

vale a dire, dell'incriminazione autonoma di tale reato, accanto a quello di istigazione, nonostante il primo sia stato da tempo trasformato in una forma di istigazione indiretta.

Pertanto, sul versante legislativo, sarebbe opportuno eliminare una volta e per tutte il riferimento all'apologia, scongiurando definitivamente i problemi di compatibilità costituzionale che questa disposizione solleva. Nonché, si potrebbe intervenire sul delitto di istigazione *ex* art. 414, 1 comma c.p., tipizzando già a livello di costruzione normativa elementi selettivi dell'area del penalmente rilevante, così da ridimensionare le odierne valutazioni arbitrarie dei giudici[70].

In attesa dell'invocata risoluzione, per via costituzionale o legislativa, non resta che fare affidamento sulla "buona coscienza" dei giudici. È, infatti, sugli organi giurisdizionali di merito e di legittimità che, in ultima istanza, viene fatta gravare la tenuta del sistema democratico, di cui i reati di opinione sono banco di prova.

L'auspicio è che il potere giudiziario riesca a valorizzare la capacità del sistema vigente di offrire efficaci risposte alla minaccia del terrorismo di matrice islamica, senza rinunciare ai principi garantistici che informano la democrazia politica ed il diritto penale sostanziale e processuale; e, ancora, che la necessità di far fronte all'allarme in questione non conduca ad affievolire la nostra identità di Stato liberale di diritto[71].

Un'ultima considerazione. Non sia soltanto il diritto penale lo strumento utilizzato per contrastare il terrorismo nelle sue inedite forme camaleontiche. Considerarlo capace di risolvere da solo il problema, come se fosse possibile attraverso la previsione di un reato eliminare il fenomeno alla radice, è illusorio e pericoloso.

Piuttosto, la difesa del nostro ordinamento da una minaccia globale di così straordinaria complessità dovrebbe servirsi – accanto all'ineludibile repressione criminale – di tutti gli strumenti disponibili per dar vita a politiche culturali di integrazione sociale che puntino a prevenire, prima ancora che a punire, l'insorgenza di radicalizzazioni che possano sfociare in fenomeni terroristici.

Proprio in questa direzione, di recente, si sono rilevati importanti segnali di apertura. Basti pensare alle numerose iniziative che promuovono e intensificano la cooperazione giudiziaria con specifico riguardo al sistema penitenziario: lo scopo è prevenire l'estremismo jihadista mediante azioni dirette non solo a eliminare le condizioni criminogene presenti in un dato contesto prima che si siano manifestati segnali di pericolo, ma anche a contenere eventuali ricadute quando l'evento criminale sia già stato commesso[72].

È questa la via maestra su cui puntare, anche nel prossimo futuro, per ridimensionare il fenomeno terroristico senza cedere a intollerabili compressioni dei diritti fondamentali.

Bibliografia

Agamben, Giorgio (2003): *Lo stato di eccezione* (Torino, Bollati Boringhieri)

Alesani, Laura (2006): *I reati di opinione. Una rilettura in chiave costituzionale* (Milano, Giuffrè)

[70] Interessante e attuale è la posizione di De Vero (1988), pp. 183 ss. e 215. L'Autore proponeva di tipizzare gli elementi di pericolosità del reato di istigazione *ex* art. 414 c.p. attraverso la previsione legislativa dell'unità di contesto-temporale dell'istigazione pubblica a commettere fattispecie previamente individuate.

[71] In realtà, come si è visto, la tendenza dominante della giurisprudenza è quella di accettare flessibilizzazioni dei succitati principi, in nome della tutela della sicurezza collettiva, spesso arretrando oltre i già affievoliti limiti delle disposizioni incriminatrici. Si distingue per l'anima – in parte – garantista, seppure non direttamente rispetto alla tipicità dell'istigazione, Cass., Sez. I, 28 giugno 2017, n. 7203.

[72] Negli ultimi anni sono state elaborate diverse iniziative sul versante penitenziario, sul presupposto che le carceri sono divenute un luogo a forte rischio di radicalizzazione. Da ultimo, va segnalato il progetto EU *Rasmorad* che ha visto l'Italia, a partire dal 2017, capofila di un piano volto a prevenire la radicalizzazione all'interno delle carceri, allo sviluppo di una metodologia di valutazione del rischio, nonché alla promozione di misure alternative al carcere. Gli esisti della ricerca scientifica, del periodo di due anni, sono stati presentati nel dicembre 2018 alla Conferenza di Roma che ha concluso i lavori e diffusi attraverso cinque moduli formativi *online* consultabili in www.rasmorad.org. Interessante è anche il progetto sperimentale antiradicalizzazione elaborato nel 2017 in collaborazione tra il Dipartimento Amministrazione Penitenziaria e l'Unione delle comunità islamiche d'Italia con destinatari otto istituti penitenziari italiani. Tali programmi hanno trovato riscontri anche sul versante legislativo: si veda la proposta di legge C. 3558-A, approvata alla Camera nel luglio 2017 e arenatasi in Senato, che prevedeva misure volte a prevenire i fenomeni di radicalizzazione e di diffusione dell'estremismo jihadista, nonché a provvedere al recupero umano, sociale, culturale e professionali di soggetti già coinvolti in fenomeni di radicalizzazione.

Bartoli, Roberto (2008): *Lotta al terrorismo internazionale tra diritto penale del nemico*, ius in bello *del criminale e annientamento del nemico assoluto* (Torino, Giappichelli)

Bognetti, Giovanni (1971): "Apologia di delitto punibile ai sensi della Costituzione e interpretazione della norma dell'art. 414 c.p., ultimo comma", *Rivista italiana di diritto e procedura penale*, pp. 18-55

Cavaliere, Antonio (2009): "Può la "sicurezza" costituire un bene giuridico o una funzione del diritto penale?", *Critica del diritto*, 1/4, pp. 43-63

Cavaliere, Antonio (2015): "Considerazioni critiche intorno al D.L. antiterrorismo, n. 7 del 18 febbraio 2015", *Diritto penale contemporaneo – Rivista trimestrale*, 2, pp. 226-235

Cerase, Marco (1993): "Sull'apologia e i reati di pericolo la Cassazione fa un salto indietro", *Cassazione penale*, 7, pp. 1715-1720

Cirillo, Paolo (2018): "Apologia della jihad islamica sul web: tra diritto penale costituzionalmente orientato e diritto penale del "nemico", *Diritto e religioni*, 2, pp.

Cirillo, Paolo (2019): "Istigazione e apologia nei recenti (dis)orientamenti giurisprudenziali", *Diritto penale e processo*, 9, pp. 1292-1302

Clemente, Antonio (2007): "Modifiche al codice penale in materia di reati di opinione a seguito della l. n. 85 del 2006", *Giurisprudenza di merito*, 1, pp. 26-35

Dambruso, Stefano (2018): *Jihad. La risposta italiana al terrorismo: le sanzioni e le inchieste giudiziarie* (Roma, Dike)

De Marinis, Francesca (2017): "Considerazioni minime intorno al tentativo di arruolamento, tra legislazione e prassi giurisprudenziale", *Diritto penale contemporaneo*, 7/8, pp. 71-78

De Vero, Giancarlo (1988): *Tutela penale dell'ordine pubblico. Itinerari ed esiti di una verifica dogmatica e politico-criminale* (Milano, Giuffrè)

Di Giovine, Alfonso (1988): *I confini della libertà di manifestazione del pensiero. Linee di riflessione teorica e profili di un diritto comparato come premesse a uno studio sui reati di opinione* (Milano, Giuffrè)

Dolcini, Emilio (2014): "Omofobi: nuovi martiri della libertà di manifestazione del pensiero?", *Rivista italiana di diritto e procedura penale*, 1, pp. 7-31

Donini, Massimo (2007): "Diritto penale di lotta. Ciò che il dibattito sul diritto penale del nemico non deve limitarsi a esorcizzare", *Studi sulla questione criminale*, 2, pp. 55-87

Esposito, Carlo (1958): *La libertà di manifestazione del pensiero nell'ordinamento italiano* (Milano, Giuffrè)

Fasani, Fabio (2015): "Le nuove fattispecie antiterrorismo: una prima lettura", *Diritto penale e processo*, 8, pp. 926-947

Fasani, Fabio (2016): *Terrorismo islamico e diritto penale* (Padova, Cooperativa Libraria Universitaria)

Fasani, Fabio (2019): "Le parole preparatorie. I reati antiterrorismo di parola nell'era dei new media", *Diritto penale contemporaneo – Rivista trimestrale*, 1, pp. 108-145

Ferrajoli, Luigi (2006): "Il "diritto penale del nemico" e la dissoluzione del diritto penale", *Questione Giustizia*, 4, pp. 797-812

Fiandaca, Giovanni e Musco, Enzo (2009): *Diritto penale. Parte generale* (Bologna, Zanichelli)

Fiandaca, Giovanni e Musco, Enzo (2012): *Diritto penale. Parte Speciale*, I (Bologna, Zanichelli)

Fiore, Carlo (1972): *I reati di opinione* (Padova, CEDAM)

Fiore, Carlo (1980): "voce Ordine pubblico", *Enciclopedia del diritto*, XXX (Milano, Giuffrè)

Flor, Roberto (2017): "Cyber-terrorismo e diritto penale in Italai", in Wenin, Roberto e Fornasari, Gabriele (eds.): *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali. Atti del convegno di Trento, 2 e 3 ottobre 2015* (Napoli, ESI), pp. 325-360

Forti, Gabrio (2016): "Le tinte forte del dissenso nel tempo dell'iper-comunicazione pulviscolare. Quale compito per il diritto penale?", *Rivista italiana di diritto e procedura penale*, 2, pp. 1034-1060

Fronza, Emanuela (2006): "Legislazione antiterrorismo e deroghe ai diritti fondamentali: riflessioni sulla teoria del "margine nazionale di apprezzamento", *Studi sulla questione criminale*, 1, pp. 31-57

Fronza, Emanuela (2016): "Criminalizzazione del dissenso o tutela del consenso. Profili critici del negazionismo come reato", *Rivista italiana di diritto e procedura penale*, 2, pp. 1016-1033

Giordano, Luigi (2019): "Associazione con finalità di terrorismo: l'interpretazione giurisprudenziale di una fattispecie problematica", *Diritto penale e processo*, 2, pp. 274-283

Gullo, Antonio (2013): *Diffamazione e legittimazione dell'intervento penale: contributo a una riforma dei delitti contro l'onore* (Roma, Aracne)

Jakobs, Gunther (2007): "Diritto penale del nemico", in Donini, Massimo e Papa, Michele (a cura di): *Diritto penale del nemico. Un dibattito internazionale* (Milano, Giuffrè), pp. 5-29

Leotta, Carmelo Domenico (2016): "La repressione penale del terrorismo a un anno dalla riforma del D.L. 18 febbraio 2015 n.7, conv. con modif. dalla L. 17 aprile 2015 n. 43", *Archivio penale*, 1, pp. 11-27

Maiello, Vincenzo (2012): "Pessina e la scuola classica", *Diritto e religioni*, 2, pp. 406-431

Marino, Giuseppe (2017): "Lo statuto del "terrorista": tra simbolo ed anticipazione", *Diritto penale contemporaneo – Rivista trimestrale,* 1, pp. 44-52

Masarone, Valentina (2013): *Politica criminale e diritto penale nel contrasto al terrorismo internazionale. Tra normativa interna, europea e internazionale*, (Napoli, Edizioni Scientifiche Italiane)

Mazzanti, Edoardo (2017): "L'adesione ideologica al terrorismo islamista tra giustizia penale e diritto dell'immigrazione", *Diritto penale contemporaneo – Rivista trimestrale*, 1, pp. 26-43

Merli, Antonella (2006): *Democrazia e diritto penale* (Napoli, Edizioni Scientifiche Italiane)

Nardi, Valérie (2016): "Quando "la parola contraria" è ritenuta penalmente irrilevante", *Diritto penale e processo*, 9, pp. 1221-1230

Nardi, Valérie (2017): "La punibilità dell'istigazione nel contrasto al terrorismo internazione", *Dirtto penale contemporaneo – Rivista trimestrale*, 1, pp. 115-131

Nicosia, Emanuele (2006): *Convenzione europea dei diritti dell'uomo e diritto penale* (Torino, Giappichelli)

Padovani, Tullio (2006): "Un intervento normativo scoordinato che investe anche i delitti contro lo Stato", *Guida al dirit*to, 14, pp. 23-31

Palazzo, Francesco (2006): "Contrasto al terrorismo, diritto penale del nemico e principi fondamentali", *Questione Giustizia*, 4, pp. 666-686

Paliero, Carlo Enrico (2012): "L'Agorà e il palazzo. Quale legittimazione per il diritto penale?", *Criminalia*, pp. 95-117

Pelissero, Marco (2000): *Reato politico e flessibilità delle categorie dogmatiche* (Napoli, Jovene)

Pelissero, Marco (2006): "Osservazioni critiche sulla legge in tema di reati di opinione: occasioni e incoerenze sistematiche", *Diritto penale e processo*, 8, pp. 859-871

Pelissero, Marco (2010): *Reati contro la personalità dello Stato e contro l'ordine pubblico* (Torino, Giappichelli)

Pelissero, Marco (2015): "La parola pericolosa. Il confine incerto del controllo penale del dissenso", *Questione giustizia*, 4, pp. 37-46

Pelissero, Marco (2016): "Contrasto al terrorismo internazionale e il diritto penale al limite", *Questione Giustizia*, pp. 99-112

Piciotti, Lorenzo (2011): "Limiti garantistici delle incriminazioni penali e nuove competenze europee alla luce del Trattato di Lisbona", in Grasso, Giovanni, Piciotti, Lorenzo, Sicurella, Rosaria (a cura di): *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona* (Milano, Giuffrè), pp. 207-232

Pulitanò, Domenico (2006): "Libertà di manifestazione del pensiero, delitti contro la personalità dello Stato e contro l'ordine pubblico (art. 21 Cost.)", in Vassalli, Giuliano (a cura di): *Diritto penale e giurisprudenza costituzionale* (Napoli, Edizioni Scientifiche Italiane), pp. 239 ss.

Pulitanò, Domenico (2015): "Di fronte al negazionismo e al discorso d'odio", *Diritto penale contemporaneo – Rivista trim*estrale, 4, pp. 325-332

Rodotà, Stefano (2013): *Il diritto di avere diritti* (Roma-Bari, Laterza)

Rossi, Chiara (2016): *L'elemento oggettivo del reato di cui all'art. 414, comma 4 c.p.*, *Cassazione penale,* 6, pp. 2466-2474

Sciarabba, Vincenzo (2006): "I diritti e i principi fondamentali nazionali ed europei e la problematica comunitarizzazione delle risoluzioni antiterrorismo dell'ONU", *Rassegna forense*, 1, pp. 147-190

Scotto Rosato, Angelo (2016): "Osservazioni critiche sul nuovo "reato" di negazionismo", *Diritto penale contemporaneo – Rivista trimestrale*, 3, pp. 280-312

Spena, Alessandro (2007): "Libertà di espressione e reati di opinione", *Rivista italiana di diritto e procedura penale*, 2/3, pp. 689-738

Stuart Mill, John (2000): *Sulla libertà* (trad. Mollica, Giovanni (a cura di), Milano, Bompiani)

Vidino, Lorenzo (2014): *Il jihadismo autoctono in Italia: nascita, sviluppo e dinamiche di radicalizzazione* (Milano, ISPI)

Viganò, Francesco (2007): "Il contrasto al terrorismo di matrice islamico-fondamentalistica: il diritto penale sostanziale", in de Maglie, Cristina e Seminara, Sergio (a cura di): *Terrorismo internazionale e diritto penale* (Padova, CEDAM), pp. 125-152

Viganò, Francesco (2017): "Un'importante pronuncia della Consulta sulla proporzionalità della pena", *Diritto penale contemporaneo – Rivista trimestrale*, 2, pp. 61-66

Visconti, Costantino (2008): *Aspetti penalistici del discorso pubblico* (Torino, Giappichelli)

Zirulia, Stefano (2015): "Apologia dell'IS via internet e arresti domiciliari. Prime prove di tenuta del sistema penale rispetto alla nuova minaccia terroristica", *Diritto penale contemporaneo,* 14 dicembre 2015

Financial cybercrime
Cibercrimen financiero
Financial Cybercrime

Crowdfounding @ ICOs: esigenze di prevenzione del rischio di commissione di reati nell'era della digital economy

Crowdfunding @ ICOs: exigencias de prevención del riesgo de comisión de delitos en la era de la economía digital

Crowdfunding @ ICOs: Commission Risk Prevention Needs of Crimes in the Era of the Digital Economy

Antonietta di Lernia
Dottoranda di ricerca in diritto penale, Università degli studi di Bari "A. Moro"
antonietta.dilernia@uniba.it

Reati informatici, Riciclaggio
Delitos informáticos, Money Laundering
Cybercrimes, Lavado de activos

Abstracts

Negli ultimi quindici anni, l'innovazione tecnologica ha rivoluzionato gli aspetti culturali e sociali e le metodologie di consumo e produzione di prodotti e servizi, trasformando il web in una possibile fonte di business per le imprese. Le "barriere" normative del processo di raccolta di capitali richiesto dalle banche e dagli intermediari finanziari abilitati hanno concorso, poi, all'affermazione di strumenti evoluti di finanziamento. Si pensi, in particolare, al Crowdfunding e alle ICOs che costituiscono strumenti di "disintermediazione" della raccolta del risparmio per finanziare, direttamente e senza intermediari, progetti con ambizioni di scala globale. È evidente che alle opportunità che questi nuovi strumenti offrono si accompagnano minacce anche molto gravi, che intercettano una preoccupante trasmigrazione di interi settori della criminalità economico-finanziaria verso lo spazio virtuale. In questa prospettiva l'innovazione tecnologica impone, oggi, al sistema penale di intraprendere un processo di "deindividualizzazione" degli strumenti di contrasto tipici, invero, di un diritto penale senza vittima che mira a proteggere interessi diffusi e astratti.

En los últimos quince años, la innovación tecnológica ha revolucionado los aspectos culturales y sociales y los métodos de consumo y producción de productos y servicios, transformando la web en una posible fuente de negocios para las empresas. Las "barreras" regulatorias del proceso de captación de capital solicitadas por los bancos y por los intermediarios financieros autorizados contribuyeron a la afirmación de instrumentos financieros avanzados. Considérese, en particular, el Crowdfunding e ICO, que son instrumentos de "desintermediación" de la recaudación de ahorros para financiar, directamente y sin intermediarios, proyectos con ambiciones a escala global. Es evidente que, junto a las oportunidades que ofrecen estos nuevos instruemntos, existen amenazas graves, que interceptan una preocupante transmigración de sectores enteros de criminalidad económica y financiera hacia el espacio virtual. Desde esta perspectiva, la innovación tecnológica exige que el sistema penal emprenda un proceso de "desindividualización" de los instrumentos de contraste típicos, de hecho, de un derecho penal sin una víctima que tenga como objetivo proteger los intereses generalizados y abstractos.

In the last fifteen years, technological innovation has revolutionized the cultural and social aspects and the methods of consumption and production of products and services, transforming the web into a possible source of business for businesses. The regulatory "barriers" of the capital raising process requested by the banks and by the authorized financial intermediaries contributed to the affirmation of advanced financing instruments.

Consider, in particular, Crowdfunding and ICOs, which are instruments of "disintermediation" of the collection of savings to finance, directly and without intermediaries, projects with global scale ambitions. It is clear that the opportunities that these new tools offer are accompanied by very serious threats, which intercept a worrying transmigration of entire sectors of economic and financial crime towards virtual space. In this perspective, technological innovation requires, today, the penal system to undertake a process of "de-individualization" of typical contrasting instruments, indeed, of a criminal law without a victim that aims to protect widespread and abstract interests.

Sommario

1. La c.d. *data platform economy*: alcune considerazioni introduttive.

"*Crowdfunding, si inverte la rotta*[1]"e "*Report SEC, esplosione e rischi delle ICOs*[2]", sono soltanto alcuni esempi dei numerosi articoli comparsi di recente sulla stampa e relativi alla crescita – a tratti anche esponenziale - del fenomeno della finanza alternativa[3].

Si tratta, invero, di un dato molto significativo se si considera che il nostro è un Paese a vocazione 'banco-centrica', e con scarsa propensione a diversificare le fonti finanziarie seguito, tuttavia, dai primi stop all'utilizzo in particolare di *Icos* da parte di Consob e autorità Svizzere al fine di apprestare un'efficace tutela degli investitori.

Come segnalato dalla stampa, recenti studi confermano che l'innovazione tecnologica digitale sta cambiando profondamente le caratteristiche strutturali dei moderni sistemi economici, favorendo l'emersione di nuovi mercati e la trasformazione radicale dei modelli di *business*, ma sta provocando anche notevoli mutamenti nei comportamenti sociali e nello stile di vita delle persone, non sempre fondati su scelte consapevoli e ragionate.

Il motore di questa trasformazione digitale dell'economia è da individuare nell'impetuoso sviluppo di piattaforme *on line* di servizi che, trasformando il *web* in una possibile fonte di *business* per le imprese motivate a raggiungere livelli competitivi e concorrenziali, assicurano facilità di comunicazione e di accesso ai mercati di scambio di beni e servizi da parte di consumatori/utenti e imprese[4].

Le "barriere" normative del processo di raccolta di capitali richieste dalle banche e dagli intermediari finanziari abilitati (art. 11-130 del Testo unico D.lgs 385/1993) hanno concorso, inoltre, all'affermazione sul mercato della neo-imprenditoria di strumenti evoluti di finanziamento per le più svariate attività.

Ci si riferisce, in particolare, al *Crowdfunding*[5] e alle *ICOs*[6] che, con alcune differenze

[1] Cucchiarato (2018).
[2] Lugano (2018).
[3] Schena *et al.* (2018), p. 8.
[4] La c.d. (*Data) Platform Economy* è una realtà adelevatissima capacità pervasiva, favorita sia dall'utilizzo di risorse infrastrutturalisempre più potenti ed elastiche (Internet, reti telematiche, Big Data, sistemi disicurezza digitale) sia dall'aumentate capacità di ricerca, elaborazione, stoccaggio etrasmissione sicura delle informazioni (Big Data analytics, machinelearning,intelligenza artificiale, cloud-computing, DistributedLedgerTechnology ecc.).
[5]Tale espressione è impiegata per indicare il finanziamento di iniziative, progetti o *start-up* da parte della folla (*crowd*) dei *web surfers* per mezzo di piattaforme *on-line.* Come più dettagliatamente e ampiamente definito da CONSOB nel Regolamento emanato nel 2013 in materia di *equity crowdfunding* (il 20 giugno 2019 la Consob ha posto in consultazione un documento recante "Modifiche al regolamento n. 18592 del 26 giugno 2013 sulla raccolta di capitale di rischio tramite portali on-line". Molte le novità che interesseranno le piattaforme di crowdfunding e che potrebbero incidere profondamente sul mercato della raccolta di capitale tramite portali web; – disponibile in http://www.consob.it/cnbarchives/documenti/Regolamentazione/lavori_preparatori/consultazione_crowdfunding_20190620.pdf -) in merito alla disciplina applicabile alla gestione dei portali on-line ed alle offerte per la raccolta di capitali, con "*il termine crowdfunding si indica il processo con cui più persone ("folla" o crowd) conferiscono somme di denaro (funding), anche di modesta entità, per finanziare un progetto imprenditoriale o iniziative di diverso genere utilizzando siti internet ("piattaforme" o "portali") e ricevendo talvolta incambio una ricompensa. [….].* Il concetto di *crowdfunding* e la sua connessione con il *crowdsourcing* è approfondito in Fregonara (2014), p. 4. In proposito inoltre, Laudonio *et al.* (2016), pp. 113-115. Deve inoltre considerarsi la recente e sempre più rilevante emersione di vere e proprie *exchange platforms* che supportano le operazioni di emissione di cripto asset.
[6]Le *Initial coin offerings (Icos*) rappresentano una particolare modalità di finanziamento di progetti imprenditoriali di vario genere che si realizzano mediante l'emissione e la successiva offerta al pubblico di *token* (*crypto-assets*) generati avvalendosi delle tecnicalità fornite dalla *Distributed ledger technology* (Dlt). I *token* qualificabili come strumenti finanziari sono allo stato assoggettati alla disciplina europea dei mercati finanziari, e l'Esma a livello Ue sta svolgendo approfondimenti relativamente alle problematiche di applicazione della citata disciplina. La grande diffusione del fenomeno delle *initial coin offerings* nel 2017, indipendentemente da considerazioni di merito sulle finalità e sulle caratteristiche di tali operazioni, denota la relativa semplicità e duttilità di utilizzo della DLT nei diversi ambiti della *securities-(trade)-life-cycle*. In considerazione della ormai ampia diffusione di operazioni c.d. di *initial coin offerings* (ICOs) e, quindi, di *crypto-asset* nelle quali investono i risparmiatori italiani la Consob ha pubblicato, il 19 marzo u.s., un Documento per la Discussione volto ad avviare un dibattito a livello nazionale sul tema delle offerte iniziali e degli scambi di cripto-attività (disponibile in http://www.consob.it/documents/46180/46181/doc_disc_20190319.pdf/64251cef-d363-4442-9685-e9ff665323cf). Il documento formula dei quesiti in merito ad un possibile approccio regolatorio. In attesa della definizione in ambito europeo di un condiviso orientamento in materia la Consob, sensibile al tema in quanto autorità deputata alla tutela degli investitori, ha ritenuto opportuno approfondire il fenomeno dei *token*, che non integrano la definizione di strumento

relative alla regolamentazione, alla piattaforma su cui si basano, alla tipologia di progetto finanziabile e al relativo valore, agli eventuali premi ed ai rischi per i contributori costituiscono entrambi strumenti di "disintermediazione" della raccolta del risparmio per finanziare, direttamente e senza intermediari, progetti imprenditoriali e tecnologici con ambizioni di scala globale.

È appena il caso di osservare che alle opportunità che questi nuovi strumenti offrono si accompagnano minacce anche molto gravi che, in misura maggiore o minore, intercettano una preoccupante trasmigrazione di interi settori della criminalità economico-finanziaria verso lo spazio virtuale.

I moderni strumenti di finanziamento, invero, sono particolarmente esposti al rischio di essere sfruttati da coloro che sono coinvolti in attività criminali come il terrorismo, lo spaccio di droga, il commercio illegale di armi, l'elusione fiscale e altri.

In questa prospettiva l'innovazione tecnologica impone, oggi, al sistema penale di confrontarsi con gli attuali scenari, elaborando soluzioni e progettando nuovi assetti di disciplina.

In relazione a queste premesse, senza avere in alcun modo la pretesa di dare conto in maniera esaustiva dei rischi significativi (o molto significativi) a cui sono esposte le attività di *Crowdfunding* e *ICOs* si cercherà, piuttosto, di valutare se l'ordinamento sia già dotato degli strumenti per contrastare i suddetti fenomeni criminali, ovvero occorra implementarlo con l'introduzione delle disposizioni anche di carattere non punitivo necessarie/utili.

Si passerà, poi, ad analizzare in particolare la *blockchain* nell'ottica della sfida che questa nuova tecnologia rappresenta rispetto ai modelli normativi tradizionali. In questo ambito, particolare attenzione sarà riservata alla verifica della corrispondenza/congruenza delle disposizioni incriminatrici più comunemente adottate con il formante empirico-criminologico del fenomeno in esame.

2. Strumenti di finanza alternativa e tutela del risparmio tra prevenzione come sistema di 'contrasto'…

Lo sviluppo tecnologico e l'applicazione informatica alla nuova finanza, congiuntamente alle difficoltà per le piccole e medie imprese di soddisfare il proprio fabbisogno finanziario (c.d. *funding gap*), ha fatto emergere inediti canali di finanziamento, idonei a ridefinire l'offerta dei servizi finanziari e il modello di *business* degli intermediari, e ad influenzare le abitudini di famiglie e risparmiatori non professionali, alla ricerca di rendimenti elevati a breve termine.

Tra questi rilevano, in questa sede - in considerazione dell'attuale maggiore rilevanza sul piano operativo - le piattaforme digitali di intermediazione creditizia/finanziaria badate su modelli di *crowdfunding*, che si caratterizzano per: a) operatività a distanza, anche *crossborder*; b) limitata o inesistente *due diligence* sugli ideatori dei progetti ovvero sui progetti stessi[7]; c) breve durata degli investimenti; d) possibilità di fenomeni di *earlyredemption* degli investimenti.

Una serie di documenti elaborati da diverse autorità nazionali e sovranazionali[8] eviden-

finanziario e che possono eventualmente configurare un prodotto finanziario, ciò anche in considerazione del crescente interesse da parte dell'industria per tali iniziative che possono rivolgersi anche al pubblico retail. Il documento fornisce, quindi, una sintetica rappresentazione del fenomeno di diffusione delle *Icos* e dei connessi aspetti di interesse per la Consob, delinea un primo esercizio di definizione degli elementi costitutivi del fenomeno in esame nonché un approccio regolatorio rispetto alle offerte di cripto-attività di nuova emissione e con riguardo alla fase della successiva negoziazione delle cripto-attività oggetto di preventiva emissione e diffusione al pubblico.

[7] Motivi economici di fattibilità sembrano non consentire di impostare, a carico dei gestori dei portali, pratiche di regolare *due diligence*, come invece accade nelle operazioni di finanza internazionale. Cfr. in proposito Isenberg (2012), p. 13.

[8] Tra questi, in ambito europeo, si segnala l'"*Opinion*"in materia di *Lending based crowdfunding* emessa dall'*European Banking Authority* (EBA): cfr. EBA/Op/2015/03, reperibile su www.eba.europa.eu, 26 febbraio 2015, par. 85, p. 23: «The risks of money laundering, terrorist financing and financial crime are primarily related to the borderless nature and potentialanonymity of borrower/lenders carrying out transactions on a peer-to-peer basis that do not require personal identification»; il document *Questions & Answers* prodotto dall'*European Securities and Markets Authority* (ESMA) in tema di prevenzione delle attività di *money laundering* e *terrorist financing* nell'ambito dell'*investment-based crowdfunding*: si veda ESMA/2015/1005, *Questions and Answers. Investment-based crowdfunding: money laundering/terrorist financing*, reperibile su https://www.esma.europa.eu, 1 luglio 2015, pp. 4-10; nonché, da ultimo, la *Relazione* SRNA (*Supra National Risk-Assessment*) sull'antiriciclaggio pubblicata dalla Commissione europea allo scopo di orientare le autoritàdegliStatimembri verso unamiglioregestione del c.d. *ML* (*Money Laundering*) *and FT* (*FinancingTerrorism*) *risk,* secondo quanto previsto dall'art. 6 della*IV DirettivaAntiriciclaggio* (Dir. 2015/849/UE): COM/2017/340, *Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, Brussels, 26 giugno 2017, 55 ss., su http://eur-lex.europa.eu/legalcontent/en/txt/?uri=com:2017:340:fin. In ambito internazionale, particolarmente degno di nota è il documento

ziano, tuttavia che, pur avendo come scopo principale il finanziamento di progetti imprenditoriali creativi, le piattaforme *on line* di *crowdinvesting* sono particolarmente esposte, a causa proprio delle summenzionate caratteristiche, ad un utilizzo abusivo da parte di organizzazioni criminali interessate a sfruttare i canali dell'economia legale a scopo di riciclaggio o di finanziamento del terrorismo.

Tra i primi rileva, in particolare, il Rapporto UIF del 18 aprile 2016[9] in cui l'Ufficio ha segnalato, tra le nuove modalità di realizzazione del finanziamento del terrorismo, la raccolta di fondi *on line* attraverso piattaforme di *crowdfunding* e il ricorso alle valute virtuali ribadendo, nel successivo rapporto per il 2017[10], che le attività di *crowdfunding* sono, nel settore finanziario, tra i comparti più esposti a rischi "significativi" o "molto significativi".

A fronte dei segnalati rischi dell'*equity based financing*[11], e richiamato, in particolare, il quadro normativo dell'*equity based crowdfunding,* emerge un sistema italiano di contrasto al riciclaggio[12]definito, nel suo complesso, nell'ultimo Rapporto FATFGAFI «maturo, sofisticato e assistito da un robusto assetto normativo e istituzionale» e, dunque, pienamente conforme agli standard internazionali[13].

L'idea base è che la circolazione della ricchezza mediante sistemi elettronici abbia progressivamente condotto a fenomeni di disintermediazione bancaria, trasferendo il luogo di incontro tra domanda e offerta di risparmio direttamente sul mercato finanziario, dove la distribuzione dei rischi avviene attraverso forme contrattuali caratterizzate da asimmetria informativa.

Ciò innesca la corrispondente richiesta di maggiore trasparenza dei rapporti di mercato, puntando a una chiara individuazione dei rischi, e sposta il baricentro dall'attività bancaria al mercato finanziario, esaltando il valore del risparmio e rendendo indispensabile la tutela ad esso garantita dall'art. 47 della Costituzione "in tutte le sue forme".

In questa ottica, assume rilievo primario la prevenzione dell'illegalità e la tutela del risparmio diventa il bene giuridico da preservare che, per sua natura richiede, evidentemente, una garanzia di carattere preventivo in considerazione della peculiarità degli interessi sovra individuali, collettivi e diffusi che vengono in rilievo, e consente alle ragioni di politica criminale di rimanere ancorate all'evoluzione di un settore estremamente 'volatile', come quello economico-finanziario evitandone, così, l'isolamento.

Eppure, a fronte del suo valore di rango costituzionale, l'esperienza pratica rivela che la tutela penale del risparmio, essendo ancorata a quella del credito, è solo indiretta e pertanto, di fronte ai nuovi prodotti finanziari, rischia di rimanere inattiva lasciando scoperta la tutela di un segmento particolarmente delicato, che più di altri meriterebbe l'attenzione del diritto penale.

La complessità insita nel naturale dinamismo dei mercati, inoltre, orienta la tutela del risparmio nell'angusta accezione patrimonialistica, inducendo il legislatore penale a sfruttare prevalentemente fattispecie avamposto quale presidio penalistico in materia bancaria e finanziaria.

La disciplina ad hoc dettata per l'*equity based crowdfunding* prevede, invero, diverse fattispecie a presidio delle riserve di attività (art. 50-quinquies TUF; artt. 7, 7-bis, 8, 22 e 23 Regolamento Consob n. 18592/2013). E, pertanto, per valutare l'abusivismo di un determinato servizio, è necessario osservarne in concreto le modalità di prestazione, per verificare che non integrino quei caratteri della professionalità e della continuità idonei ad assumere rilevanza penale.

---

prodotto nell'ottobre 2015 da parte del *Gruppo di azione finanziariainternazionale* (GAFI-FAFT)172, in cui, anche attraverso casi studio, sono enucleate particolari modalità di utilizzo di piattaforme *on-line* di *crowdfunding*a scopi di finanziamento del terrorismo: cfr.*Report* GAFI del 2015 *"EmergingTerroristFinancingRisks"*, reperibile al sito: www.fatfgafi.org/publications/methodsandtrends/documents/emergingterrorist-financing-risks.html. Le indicazioni ivi contenute, oltre ad aver ispirato la più recente normativa europea in materia di contrasto al finanziamento del terrorismo e al riciclaggio di proventi da reato, sono state fatte proprie, in ambito nazionale, dalla Comunicazione del 18 aprile 2016 dell'Ufficio di Informazione Finanziaria per l'Italia (UIF).

[9] *Unità di Informazione Finanziaria per l'Italia, Prevenzione del finanziamento del terrorismo internazionale*. Sia consentito il richiamo a di Lernia (2017).

[10] *Rapporto Annuale dell'Unità di Informazione Finanziaria per l'Italia*, nr. 9, Anno 2017.

[11] Schena (2018), pp. 48-51.

[12] Per una efficace ricostruzione del *framework* legale di contrasto all'indebito utilizzo di piattaforme di crowdinvesting per scopi di riciclaggio e finanziamento del terrorismo cfr. Palmerini (2018), pp. 70-73.

[13] Il Rapporto e la sua sintesi sono pubblicati sul sitodel GAFI (http://www.fatf-gafi.org/countries/d-i/italy/documents/mer-italy-2016.html). Una traduzione (non ufficiale) in lingua italiana è stata predisposta dalla V Direzione del Dipartimento del Tesoro (http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/prevenzione_reati_finanziari/rapporto_di_valutazione_aml-cft_-_versione_in_italiano.pdf).

Per un giudizio di sostanziale liceità, quindi, è necessario che i diversi portali si limitino allo svolgimento di una funzione non istituzionale di gestione o di intermediazione nei contatti tra privati; in altri termini, è essenziale che la fonte del rapporto tra gli utenti sia una relazione diretta e privatistica (riconducibile, ad esempio, allo schema della donazione, semplice e remuneratoria o, più frequentemente, del mutuo).

In questa prospettiva, l'interesse del legislatore è apparentemente sbilanciato sull'incriminazione (e repressione) dell'abusivismo, puntando a garantire l'affidabilità dei mercati mediante la qualità dei suoi attori-protagonisti.

Ne risulta una fotografia della tutela penalistica concentrata quasi esclusivamente sull'accesso ai diversi segmenti del mercato finanziario, dove la sanzione penale presidia la generale "riserva di attività", e rende l'attuale diritto penale dei mercati finanziari un importante tassello nelle strategie di contrasto alla criminalità organizzata e uno strumento essenziale nella lotta all'infiltrazione della stessa all'interno dell'economia legale.

3. …e repressione. In particolare, il riciclaggio ed il finanziamento del terrorismo.

I nuovi strumenti di finanza alternativa, generati e diffusi dal *web*, il non luogo, il meta-territorio, appaiono indissolubilmente legati alle relative fortune e meccaniche.

Data la sconfinatezza del *world wide web* risulta, a tutt'oggi, sempre più complessa l'attività volta a contrastare fenomeni illeciti, capaci di alterare i circuiti legali dell'economia e della concorrenza.

Si osserva, al riguardo, che le transazioni finanziarie sono operazioni molto pericolose, poiché permettono di effettuare movimenti di fondi senza un rapporto diretto con i clienti rimanendo, così, anonimi i soggetti di ogni singola transazione. Le operazioni effettuate in *internet*, inoltre, sono sviluppate concretamente in diversi ordinamenti giuridici, alcuni dei quali non prevedono adeguate misure antiriciclaggio.

Di recente, alcuni studi hanno evidenziato che i nuovi strumenti di finanza alternativa, proprio a causa dei loro caratteri principali, aprono inquietanti scenari circa i possibili rischi di riciclaggio[14] e finanziamento del terrorismo[15].

Per comprendere tali rischi, basti pensare che gli interventi di contrasto alle transazioni illecite si sviluppano con indagini di polizia giudiziaria, con l'approfondimento delle segnalazioni di operazioni sospette inoltrate da intermediari ed operatori finanziari, e con i controlli sulle movimentazioni di valuta.

Non meno importanti sono, poi, le ispezioni ed i controlli nei confronti dei destinatari della normativa antiriciclaggio (intermediari finanziari, money transfer, società fiduciarie, ecc.), con lo scopo di verificare il corretto adempimento dei relativi obblighi (adeguata verifica della clientela, registrazione dei dati e segnalazione delle operazioni sospette), e prevenire l'utilizzo del sistema finanziario per movimentare capitali di origine illecita.

Anche se i sostenitori della *blockchain* - concentrati sul relativo potenziale - ne pongono in secondo piano i possibili pericoli, concretamente riscontrabili in assenza di intermediari finanziari, le operazioni di *crowdfunding* basate su tale tecnologia, proprio a causa del principale vantaggio, strettamente legato al relativo funzionamento - che consiste nell'agevolare la disintermediazione dei flussi finanziari – sono particolarmente esposte a tali rischi.

I sottoscrittori che conferiscono somme di denaro, anche modeste, per finanziare un progetto, invero, potrebbero impiegare somme provenienti da delitto. Potrebbero sussistere, inol-

[14] Il riciclaggio di denaro può essere descritto come l'attività di riutilizzo del denaro "sporco" in attività legali, al fine di mascherarne la provenienza illecita. Il processo di riciclaggio si lascia descrivere in tre fasi. La prima fase di "piazzamento" (placement) dei proventi illeciti nel mercato interno o internazionale serve a collocare provvisoriamente i beni lontano dal locus commissi delicti, in modo da ostacolare eventuali attività d'indagine. Segue la seconda fase di "stratificazione" (*layering*), finalizzata a predisporre plurimi strati documentali idonei ad ostacolare il paper-trail, in particolare mediante operazioni finanziarie (es. trasferimenti internazionali di fondi, operazioni societarie in paesi off-shore etc.). Infine, per mezzo della c.d. "integrazione" (*integration*), i proventi ormai puliti vengono immessi in bacini di giacenza di capitali di origine lecita o in circuiti economico-finanziari legali.

[15] Il finanziamento del terrorismo, al contrario, può avere come fonte anche attività lecite. L'origine non necessariamente illecita delle disponibilità nonché l'utilizzo di somme spesso di importo esiguo rendono particolarmente complessa l'individuazione preventive delle condotte finalizzate a finanziare il terrorismo. Inoltre, il network terrorista sfrutta abilmente le potenzialità offerte dall'integrazione a livello globale dei mercati al fine di veicolare, da un Paese all'altro, i fondi essenziali per la propria attività.

tre, accordi collusivi tra ideatori del progetto e investitori, o tra i gestori delle piattaforme e gli stessi investitori, ad esempio per occultare l'origine illecita dei fondi.

Per raccogliere capitale di rischio, infatti, è possibile effettuare le operazioni sopra descritte che sfruttano il potere della rete di decidere in cosa e come investire, e decentralizzano i meccanismi di controllo al fine di ottenere più trasparenza e 'democrazia finanziaria', grazie soprattutto alle reti *peer-to-peer* tra i soggetti che ne sono coinvolti[16].

Dubbi sono emersi in dottrina, in particolare, in ordine alla sussumibilità delle operazioni di *crowdfunding* effettuate con tecnologia *blockchain* nella fattispecie di riciclaggio.

E' opportuno, al riguardo, precisare che nell'attuale contesto normativo italiano le piattaforme di *marketplace lending* – i.e. di *crowdfunding* - non sono, come tali, soggette alla disciplina antiriciclaggio, non rientrando in alcuna delle categorie di soggetti obbligati a conformarsi a tale disciplina, previste dall'art. 3 del d.lgs. 21 novembre 2007, n. 231[17].

Si deve, tuttavia, segnalare che la scelta del legislatore italiano non è imposta dalla Direttiva antiriciclaggio, la quale non preclude agli Stati membri la possibilità di estendere l'ambito di applicabilità della relativa normativa a «categorie di imprese diverse dai soggetti obbligati di cui all'articolo 2, par. 1, le quali svolgono attività particolarmente suscettibili di essere utilizzate a fini di riciclaggio di denaro o di finanziamento del terrorismo»[18].

Si precisa, al riguardo, che la mancata estensione della disciplina di cui si discute alle piattaforme di *crowdfunding* non comporta che le stesse siano esenti dagli obblighi antiriciclaggio, i quali si applicano loro (non in quanto piattaforme, appunto, ma) in quanto soggetti a vario titolo "regolati", in conformità con il rispettivo status regolamentare.

Più precisamente, sono sottoposte in modo pieno alla disciplina antiriciclaggio le piattaforme gestite da banche, intermediari finanziari e IP italiani, e da succursali di banche ed enti finanziari comunitari.

È importante sottolineare, inoltre, che gli obblighi antiriciclaggio – a differenza degli obblighi di trasparenza – devono essere osservati da tali soggetti a prescindere dal fatto che essi svolgano un'attività finanziaria "regolata" o meno. Ad esempio, l'obbligo di adeguata verifica della clientela si applica, tra gli altri, in occasione dell'instaurazione di qualsiasi "rapporto continuativo" (art. 17, comma 1, lett. a), del d.lgs. n. 231/2007), e l'obbligo di segnalazione di un'operazione sospetta scatta in tutti i casi nei quali il soggetto obbligato ricavi elementi di sospetto, tra le altre, dalle informazioni conosciute "in ragione delle funzioni esercitate", senza alcuna limitazione (art. 35, comma 1, del d.lgs. n. 231/2007).

Si può quindi concludere che, pur in assenza di una disciplina *ad hoc,* tutte le piattaforme di *crowdfunding* che attualmente operano in Italia sono sottoposte alla normativa antiriciclaggio a causa del loro status regolamentare, ancorché a titolo diverso e con un diverso livello di coinvolgimento e di responsabilità (anche sul piano sanzionatorio).

Secondo un'opinione ampiamente condivisa, il rischio di riciclaggio connesso alle piattaforme di crowdfunding, che può aumentare in presenza di diversi fattori, può essere mitigato da un sistema caratterizzato da una governance dotata di adeguati presidi e controlli in materia di antiriciclaggio, che si tradurrebbero in obblighi di adeguata verifica di tutti i soggetti coinvolti nell'attività di finanziamento, riducendo il rischio di riciclaggio.

Le considerazioni che precedono inducono a ritenere che, anche con riferimento ai profili antiriciclaggio, sia necessario un intervento normativo ad hoc che assoggetti espressamente le piattaforme alla relativa disciplina, sia pure nei limiti richiesti dalla natura e dall'entità dei rischi cui le piattaforme stesse sono esposte, in applicazione del principio di proporzionalità, sancito tanto dall'art. 8, par. 1, della direttiva su citata, quanto dal d.lgs. n. 231/2007[19].

Essenziale, poi, è contrastare e prevenire il finanziamento del terrorismo, evitando che il *deep web*[20] - ovvero la parte di internet che si nasconde al di sotto del *web* in cui si è abituati

[16] Esempi di soluzioni di raccolta di *crowdfunding* basate sulla tecnologia *blockchain* sono Swarm, Koinify e WeiFund.

[17] Come modificato dal d.lgs. 25 maggio 2017, n. 90, di recepimento della IV Direttiva Antiriciclaggio - direttiva UE 2015/849 del 20 maggio 2015 - e che ha anticipato alcune delle novità introdotte dalla V Direttiva - direttiva UE 2018/843 -205, in corso di recepimento nel nostro Paese.

[18] Avvalendosi di tale opzione nazionale, alcune delle normative speciali nazionali in materia di crowdfunding sopra esaminate hanno operato l'estensione di cui trattasi. In particolare, la Francia ha assoggettato le piattaforme alla disciplina antiriciclaggio, mentre Regno Unito, Spagna e Portogallo hanno inserito all'interno delle rispettive discipline sul crowdfunding disposizioni che impongono semplicemente un (più o meno) generale obbligo di prevenire il riciclaggio e il finanziamento del terrorismo attraverso misure adeguate.

[19] Cfr., tra gli altri, gli artt. 2, comma 2, 14, comma 4 e 16, comma 3 della direttuiva antiriciclaggio.

[20] A differenza del *web* tradizionale, il *deep web* (o *web* "invisibile") è costituitodall'insieme di siti e servizi non rintracciabili con i normali motori di ricerca evisitabili solo sfruttando la rete di anonimizzazione. Cfr., sul punto, Spagnuolo (2014).

a navigare - in quanto territorio poco noto e inaccessibile (servono, infatti speciali software per accedere), favorisca lo svolgimento di operazioni illecite, in particolare in quella porzione detta *dark web*.

Evidentemente, non tutto questo web 'nascosto' è implicato in transazioni illegali (sono infatti presenti anche ricercatori d'avanguardia e dissidenti dei regimi totalitari) ma ciò che è certo è che, essendo territorio fertile per gli *hacker* provenienti da tutto il mondo, che comunicano al suo interno seguendo la regola del *peer-to-peer*, le operazioni risultano difficilmente tracciabili e sfuggono con facilità ai controlli.

Ciò è emerso dagli studi di una fonte dell'intelligence israeliana, i quali hanno dimostrato che i fondamentalisti islamici dell'*ISIS* sembrano conoscere e sfruttare al meglio i nuovi trend digitali, a tal punto da utilizzare il *Bitcoin* – ovvero la valuta virtuale fondata sulla tecnologia *blockchain* - come mezzo per il finanziamento delle attività e il reclutamento degli adepti.

Recenti evoluzioni nel panorama mondiale (riconosciute anche dalle Nazioni Unite), inoltre, hanno evidenziato la crescente convergenza tra criminalità organizzata e terrorismo, il cui intreccio costituisce un'accresciuta minaccia.

Del resto, già il 2 febbraio 2016, la Commissione europea aveva inviato a Parlamento europeo e Consiglio una comunicazione[21] in cui si rilevava come recenti attentati, perpetrati nell'Unione europea e nel resto del mondo, facessero emergere la necessità, per l'UE, di mettere in atto politiche di ogni genere per prevenire e combattere il terrorismo, basate su una serie di rimedi, ovvero: tagliare le fonti di finanziamento, rendere più difficile la possibilità di non essere individuati quando si usano questi fondi, e utilizzare in modo ottimale ogni informazione derivante dal processo di finanziamento.

E' accaduto più volte, inoltre, in passato che i gruppi terroristici abbiano sfruttato la falla del sistema - precedente alla riforma - rappresentata dalla mancata soggezione dei prestatori di servizi di cambio tra valute virtuali e valute aventi corso legale, ed i prestatori di servizi di portafoglio digitale all'obbligo attualmente vigente nell'Unione Europea di individuare e segnalare le attività sospette, movimentando ingenti flussi finanziari nel più totale anonimato, e dissimulando i trasferimenti con scambi tra valute virtuali[22].

Eppure, a ben vedere, neanche l'inclusione dei prestatori di servizi di scambio valuta e di portafoglio digitale nel novero dei soggetti obbligati alle segnalazioni ed al contrasto del fenomeno previsti dalla direttiva 2015/849 sembra poter risolvere, almeno potenzialmente, il problema nel suo complesso.

L'anonimato fornito da questi sistemai virtuali è garantito, infatti, a prescindere dalla presenza sul mercato degli intermediari, atteso che le operazioni di scambio avvengono tramite meccanismi di natura strettamente privata e non collettiva.

L'unico modo, peraltro auspicato dal legislatore europeo, per contrastare l'anonimato fornito da queste valute virtuali potrebbe essere la possibilità per le singole FIU – i.e. le Unità di Informazione Finanziaria nazionali - di ottenere informazioni che consentano di associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta.

Si impone, ad ogni modo, la necessità - in sede applicativa - di un controllo critico sull'incriminazione mediante il paradigma dell'offesa dell'interesse tutelato, stabilizzando la dialettica tra bene e offensività che dovrà ispirare il legislatore in prospettiva *de lege ferenda*, assicurando forme di tipizzazione che possano essere accertate mediante il controllo critico delle conseguenze della violazione.

Poste queste premesse, si ritiene che la standardizzazione delle infrastrutture sia fondamentale per prevenire l'utilizzo del sistema di pagamento internazionale ai fini di riciclaggio di denaro e finanziamento del terrorismo, dato che l'uniformità permette la tracciabilità dei flussi dei fondi e delle informazioni coinvolti nella singola transazione.

Al fine di individuare una precisa strategia di regolamentazione, è opportuno partire dal definire i fattori di rischio presenti nel concetto stesso di strumenti di finanza alternativa, che derivano necessariamente dalla loro difficile tracciabilità e sostanziale aleatorietà della trasmissione.

Si ritiene utile, infine, proporre un quadro concettuale per regolamentare le transazioni finanziarie *on line* fondato, a mero titolo esemplificativo, sulla imposizione di costi su quelle caratteristiche delle stesse che le rendono particolarmente esposte ad un comportamento cri-

[21] COM(2016) 50 final.

[22] Da questa constatazione di politica criminale, è sorta l'esigenza di modificare ed ampliare l'ambito di applicazione della direttiva 2015/849, in modo da includere tali prestatori di servizi di scambio e di portafoglio digitale nel novero dei soggetti obbligati agli obblighi antiriciclaggio.

minale (in particolare, l'anonimato), al fine di renderle sistematicamente meno idonee per un uso illecito.

4. Spunti di riflessione *de iure condendo*.

L'era digitale ha creato un mondo che si muove in parallelo rispetto a quello reale: è il *web*, senza confini e limiti temporali, dove tutto può arrivare ad essere gestito in maniera pressoché anonima.

D'altronde, più complessa diventa la società nelle sue articolazioni, più complessa tende a diventare la criminalità che ne riproduce le patologie.

In questa prospettiva, è agevole osservare che gli autori di crimini economici possiedono competenze specifiche al passo con il progresso tecnologico, e la finanziarizzazione della criminalità economica ha innescato un processo di de-individualizzazione degli strumenti di contrasto, tipici di un diritto penale senza vittima che mira a proteggere interessi diffusi e astratti grazie al quale non solo gli oggetti del reato, ma anche gli autori delle condotte criminali sono divenuti invisibili.

Tale osservazione giustifica l'idea, che sta iniziando a farsi strada nella società contemporanea, secondo cui alle autorità competenti serviranno nuovi e adeguati strumenti per far fronte a questo scenario 'digitale'.

In particolare, i nuovi strumenti di finanza per diventare veramente alternativi rispetto a quelli classici dovranno essere in grado di implementare i vantaggi della 'catena di blocchi', e di rendere sempre più la rete come il meccanismo peer-to-peer di 'autodifesa' delle transazioni.

Passando ad esaminare l'ultimo profilo evidenziato, ovvero il rapporto tra *regulation* e diritto penale al fine di indagare quali sono i residui spazi per un intervento penalistico in materia si osserva, in generale, che tale tema permea l'intero dibattito sul Fin-Tech.

In primo luogo, si discute della effettiva opportunità di una regolamentazione; e, risolto positivamente questo interrogativo, della tipologia e delle modalità della regolamentazione medesima.

Gli interpreti più sensibili hanno colto la problematicità di questo punto evidenziando come se una regolamentazione è necessaria od opportuna, questa non potrà non tenere conto della natura intrinsecamente integrata del mercato dei servizi offerti tramite Fin-Tech, che è per natura unitario.

Da questa considerazione, e da quella ulteriore, che si risolve nella constatazione che, in linea di principio, attraverso le nuove tecnologie vengono forniti servizi aventi il medesimo oggetto di quelli già resi attraverso le modalità "tradizionali", sorge l'affermazione del paradigma della c.d. neutralità tecnologica, che si esprime nel brocardo stessi servizi, stessi rischi, stesse regole, stessa vigilanza.

Dal momento, cioè, che la strada di una regolamentazione specifica del fenomeno FinTech non sarebbe percorribile né, sotto altro aspetto, efficace, si perviene alla conclusione che, laddove vengano svolte le medesime attività, dovrebbero poter continuare ad operare le medesime regole. Alla stregua di questo principio, dunque, le regole sarebbero tendenzialmente le medesime (se mai operando diversamente il paradigma della "proporzionalità"): ma si tratta di una raffigurazione realisticamente prospettabile?

Sotto altro profilo, la constatazione della natura del Fintech porta inevitabilmente a dover ripensare i modelli di vigilanza, conducendo ad un tramonto più o meno definitivo del modello per soggetti.

Di qui un appunto ulteriore: il problema dei regolatori, o, ancor meglio, della pluralità dei regolatori.

Il diverso "taglio" ed il diverso approccio di regolatori diversi rispetto ad un problema che si vuole unitario (se non altro sotto il profilo del mercato su cui il fenomeno produce il proprio impatto) non può non essere concepito come una "discrasia" di sistema.

Quello che appare chiaro, quindi, è che l'approccio regolatorio che eventualmente venisse adottato dovrà tenere conto del carattere disomogeneo del fenomeno – e quindi dovrà essere caratterizzato da un notevole livello di adattabilità e di proporzionalità, oltre che di gradualità – dovrà avere un carattere di sufficiente univocità ed integrazione non potendo essere condizionato da differenti approcci regolatori, e dovrà da ultimo avere il carattere transnazionale7, alla luce della natura "intrinsecamente cross-border" dei servizi prestati.

In prospettiva *de iure condendo*, occorrerebbe prevedere interventi legislativi di riforma che siano meglio in grado di intercettare le questioni relative al *FinTech*, posto che la normativa vigente non sempre si mostra sufficientemente flessibile per adeguarsi in modo tempestivo al progresso tecnologico.

In particolare, sarà fondamentale valutare se la disciplina in materia di riciclaggio, terrorismo e abusivismo possa dirsi proporzionata – quanto alla repressione, ma anche sul versante degli obblighi di carattere preventivo – rispetto alla concreta realtà dei servizi di finanza tecnologica offerti da operatori non istituzionali.

E', ormai, generalmente condivisa la necessità che i poteri pubblici raccolgano le sfide poste dai nuovi strumenti di finanza alternativa, elaborando un quadro giuridico che favorisca la continua innovazione e la relativa crescita economica, e preveda le derive peggiori accompagnando i rapidi e significativi cambiamenti che la digitalizzazione sta producendo, in particolare nel settore dei servizi finanziari.

Sarebbe opportuno, inoltre, che si trattasse di una regolazione ispirata da una buona dose di realismo, che eviti di confinare le innovazioni e le relative tecnologie nei meandri di un poco raccomandabile *deep web* nonché, considerata la transnazionalità dei fenomeni di cui ci si occupa, da volontà di armonizzazione al fine di frapporsi in modo efficace ed efficiente, in termini preventivi e repressivi, rispetto alle condotte illecite.

Per quanto attiene più in particolare il sistema penale, appare tendenzalmente condivisibile l'orientamento che sta emergendo tra gli studiosi della materia, teso ad evidenziare la necessità di un intervento *ad hoc* nella consapevolezza della specificità ed estrema delicatezza delle attività coinvolte.

Se tutela penale dovrà esserci è pressoché inevitabile il ricorso a forme di anticipazione della soglia di punibilità, a presidio degli snodi cruciali della *safety net* normativa.

È auspicabile che il legislatore si sottragga alle suggestioni di un intervento meramente simbolico e agisca con la consapevolezza che non compete al diritto penale né la prima e nemmeno la sola *ratio* dell'intervento regolatorio, spetti o meno alle pene di fornire un contributo, certamente non esclusivo, all'affermazione e stabilizzazione di un "minimo etico" nella vita degli affari.

Bibliografia

Accettella, Filippo, Ciocca, Paolo (2017), "Emittente e portale nell'equity-based crowdfunding", *Giurisprudenza Commerciale*, 1, pp. 237-251.

Aragona, Valentina (2017), "Il contrasto al finanziamento del terrorismo", *Diritto penale contemporaneo – Rivista trimestrale*, 1, pp. 96-106.

Bandiera, Barbara (2017), "FinTech e antiriciclaggio", in Paracampo, Maria Teresa: *FinTech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari* (Torino, Giappichelli), pp. 259-276.

Castrataro, Daniela, Pais, Ivana, *Analisi delle piattaforme di crowdfunding italiane,* in https://crowdfunding-news.blogspot.com/

Cucchiarato (2018), *Crowdfunding, si inverte la rotta, Italia oggi sette*, N. 273, p. 4.

di Lernia, Antonietta (2017), *Il rapporto dell'Unità di Informazione Finanziaria per l'Italia per l'anno 2016. L'approccio proattivo dell'UIF nella prevenzione al finanziamento del terrorismo*, *Dir. Pen. Cont.*.

Fregonara, Elena (2014), "Il crowdfunding: un nuovo strumento di finanziamento per le start up innovative", *Orizzonti del diritto commerciale*, 1, pp. 1-26.

Giudici, Giancarlo *et al.* (2018), *Quaderno di Ricerca La Finanza Alternativa per le PMI in Italia*, in https://www.osservatoriocrowdinvesting.it/

Girino, Emilio (2014), "Le regole del crowdfunding", *Amministrazione e Finanza*, 1, pp. 75-82.

Isenberg, Daniel (2012), "The Road to Crowdfunding Hell", in https://hbr.org/2012/04/the-road-to-crowdfunding-hell

Laudonio, Aldo, Colurcio Maria (2016), "La folla e l'impresa", (Bari, Cacucci).

Lugano, Francesco (2018), *Report SEC, esplosione e rischi delle ICO*, in https://cryptonomist.ch/

Padovani, Tullio (1995), "Diritto penale della prevenzione e mercato finanziario", *Riv. it. dir. proc. pen*., pp. 634-636.

Palmerini, Erica et al. (2018), *Quaderni FinTech n. 2. Il FinTech e l'economia dei dati. Considerazioni su alcuni profili civilistici e penalistici. Le soluzioni del diritto vigente ai rischi per la clientela e gli operatori*, in https://consob.it

Schena, Cristiana et al. (2018), *Quaderni FinTech n. 1. Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale,* in https://consob.it

Spagnuolo, Eugenio (2014), *Cinque cose da sapere sul Deep Web*, in www.focus.it

La tutela penale del segreto commerciale in Italia. Fra esigenze di adeguamento e possibilità di razionalizzazione

La tutela penal del secreto comercial en Italia. Entre exigencias de adecuación y posibilidades de racionalización

The Protection of Trade Secret under Italian Criminal Law. Between Needs for Adequacy and Options for Rationalization

Riccardo Ercole Omodei
Borsista post-doc in Diritto penale presso l'Università di Palermo
riccardoercole.omodei@unipa.it

Inviolabilità dei segreti, Interpretazione della legge

Inviolabilidad de los secretos, Interpretación legal

Inviolability of secrets, Legal Interpretation

Abstracts

Il contributo si concentra sulla disciplina penale italiana in materia di segreto commerciale, e ha l'intento di verificare se la recente riforma legislativa (D. Lgs. n. 63/2018) sia riuscita a conformare l'ordinamento domestico alle moderne istanze della *data-driven economy*. La novella ha modificato la struttura e l'oggetto di tutela dell'art. 623 c.p., e ha comportato inoltre un avvicinamento della disciplina penale al sistema di tutela civilistico predisposto dal codice della proprietà industriale (art. 98 c.p.i.). Tale avvicinamento pone all'interprete non pochi dubbi in merito alla compatibilità tra le due forme di protezione, dubbi enfatizzati dalla recente giurisprudenza convenzionale. In conclusione, si tenterà di dimostrare come, nonostante i rischi derivanti dal cumulo delle diverse discipline, permangano spazi di lecito intervento penale in materia, specialmente se si struttura in modo differente l'oggetto del segreto commerciale tutelabile dalle due diverse branche del diritto.

El presente trabajo aborda la regulación penal italiana en material de secreto comercial, a fin de verificar si la reciente reforma legislativa (D. Lgs. n. 63/2018) logró adecuar el ordenamiento nacional a las modernas instancias de la *data-driven economy*. La reciente intervención legislativa modificó la estructura y el objeto de tutela del artículo 623 del Código Penal italiano, comportando una aproximación de la regulación penal al sistema de tutela civil, previsto en el Código de Propiedad Industrial (artículo 98). Tal acercamiento plantea dudas respecto a la compatibilidad entre las formas de protección, las cuales se ven reforzadas por la reciente jurisprudencia de la Corte Europea de Derechos Humanos. Sin perjuicio de los riesgos relacionados con la superposición entre ambas regulaciones legales, el presente artículo intenta diferenciar la noción de secreto comercial en las dos ramas del derecho con la finalidad de demostrar la necesidad de la protección penal del secreto comercial.

The paper focuses on the Italian criminal provisions regarding trade secret. It aims at analyzing the consistency between the criminal law system (recently reformed by D. Lgs. N. 63/2018) and the modern needs of data-driven economy. D. Lgs. n. 63/2018 modified the structure and the object of protection of art. 623 c.p. and it also filled the gap between the criminal law system and the civil law protection (art. 98 industrial property code). Problems regarding the compatibility of the different forms of protection may arise from this reform, as underlined by the case law of the ECHR too. Notwithstanding the risks related to the overlapping of the two regulations, the paper tries to differentiate the notion of trade secret of the two branches of law in order to demonstrate the need of the criminal protection of trade secret.

Sommario

1. Premessa: il segreto commerciale nell'era della *data-driven economy*.

La centralità del segreto nel settore industriale e commerciale non è fattore caratteristico della contemporaneità, ma affonda le sue radici nel passato, in periodi ben antecedenti la rivoluzione industriale. L'esigenza di tutelare la segretezza delle prassi commerciali e mercantili era infatti già avvertita in epoca medievale, ed era anzi talmente pressante da modellare l'intero sistema economico, il cui conformarsi per il tramite di rigide corporazioni, estremamente chiuse allo sguardo esterno, assolveva al precipuo compito di assicurare la riservatezza delle informazioni e delle tecniche nei vari settori; strumento necessario per l'affermazione e la sopravvivenza del ceto mercantile[1]. A ciò si aggiunga che l'attività di spionaggio latamente intesa, secondo un adagio forse non particolarmente felice ma di sicuro effetto, è descritta nella letteratura anglosassone come la *world's second oldest profession*[2], rendendo di fatto l'esigenza di tutela del segreto connaturata alla stessa storia dell'uomo.

È però con l'incessante progredire dell'industria e del commercio che le peculiari tecniche e prassi di produzione divengono frequente obiettivo dell'altrui condotta illecita, rendendo al contempo il sempre più redditizio segreto relativo alle attività economiche oggetto specifico di tutela anche penale. Se la centralità del segreto negli scambi commerciali può considerarsi una costante della storia più o meno recente, altrettanto non può dirsi riguardo al contenuto del segreto stesso. Questo è andato variando notevolmente nel corso del tempo, seguendo di pari passo i mutamenti che hanno contraddistinto la struttura economica ed industriale della società umana. A ben guardare, però, pur mutando nel corso dei decenni il contenuto specifico del segreto protetto, non cambiava la *ratio* sottostante la scelta dell'oggetto di tutela: ciò che doveva rimanere riservato era l'informazione/la tecnica/la prassi capace di assicurare all'imprenditore/mercante/industriale un vantaggio competitivo, e quindi un'aspettativa di un maggiore profitto economico. Ad esempio, il modello di tutela penale della Francia, già industrializzata, di metà ottocento, che ha ispirato la quasi totalità delle normative euro-continentali, ha contemplato il segreto quale vero e proprio segreto di fabbrica (*secret de fabrication*)[3], tutelato, dunque, guardando al lavoratore quale veicolo esclusivo (o comunque principale) di rivelazione delle conoscenze sensibili. A sua volta, il mondo anglosassone, caratterizzato da un'economia più dinamica, successivamente ha dato rilevanza al vero e proprio *trade secret* (segreto commerciale), portando lo sguardo oltre lo steccato della fabbrica e della produzione industriale.

Da quanto appena accennato, emerge il notevole impatto che la tecnologia ha nel settore in questione, sul quale produce un duplice effetto. Da un lato, con il progredire economico muta, come già visto, l'oggetto di ciò che l'ordinamento intende tutelare, pur rimanendo immutata la sua caratteristica peculiare: l'essere l'informazione dotata di un valore strategico per l'impresa. Dall'altro, variano notevolmente i metodi di aggressione alla riservatezza in materia economica, costantemente esposta a nuove forme di minacce. In un ambito del diritto così sensibile allo sviluppo tecnologico, è facile prevedere l'impatto della dirompente, e a tratti devastante, rivoluzione digitale. A mutare profondamente è l'oggetto di ciò che costituisce ricchezza: non più il manufatto, il prodotto, il servizio ma piuttosto il dato, l'informazione. È ormai di dominio comune l'idea secondo la quale la "conoscenza è la valuta della nuova

[1] Per una ricostruzione storica della rilevanza del segreto nell'ambito economico, cfr. Mazzacuva (1979), p. 7 s.; Alessandri (1984), p. 78 s.
[2] Williams (2011), p. 1162.
[3] Sul punto cfr. Alessandri (1984), p. 103 s.

economia"[4], tanto che ogni attività economica, soprattutto se diretta all'innovazione, viene oggi concepita come necessariamente fondata su una scrupolosa attività di raccolta e analisi di dati ed informazioni. Secondo quanto indicato dall'*impact assessment* che ha accompagnato la proposta della Commissione poi confluita nella Direttiva (UE) 2016/943, nelle economie occidentali i beni immateriali (*intangible assets*), definiti come quelle informazioni valutabili ed innovative processate da un'impresa secondo uno specifico metodo e non disponibili alle altre compagnie o alla società nel suo complesso, costituiscono la maggiore fonte di investimento delle imprese, superiore agli investimenti effettuati sul capitale fisico[5], e che nelle compagnie ad alta innovazione tale quota di impegno finanziario ammonta a circa il 70/80% del valore totale.

In una c.d. *data-driven economy*, in cui la raccolta e l'uso dei dati è centrale per la gestione e lo sviluppo dell'attività d'impresa, il segreto giuridicamente rilevante non può far altro che assecondare le richieste ed esigenze degli agenti economici, fuoriuscendo definitivamente dall'esclusivo ambito della fabbrica e dell'applicazione industriale per abbracciare le nuove forme di creazione della ricchezza.

Il presente contributo intende verificare se, in un contesto come quello appena delineato, l'ordinamento italiano sia riuscito a conformarsi alle moderne istanze del settore economico. Nell'indagare se il nostro sistema penale abbia saputo aggiornare coerentemente con gli interessi coinvolti l'oggetto di tutela delle fattispecie astratte, includendo altresì le nuove modalità di aggressione, si tenterà di delineare i difficili rapporti che in tale settore intercorrono tra il sistema civilistico di protezione e quello repressivo/penalistico. Si cercherà di dimostrare come la tutela civile apprestata nell'ambito del segreto commerciale presenti oggi non poche affinità con il sistema di pene private delineato dal D. Lgs. n. 7/2016, e che tale vicinanza costituisca fonte di possibili indebite interferenze, alla luce soprattutto della definizione di materia penale delineata dalla giurisprudenza convenzionale. Nonostante i rischi derivanti dal cumulo delle diverse discipline, come si affermerà in conclusione, permangono spazi di lecito intervento penale in materia, specialmente se si struttura in modo differente l'oggetto del segreto commerciale tutelabile dalle due diverse branche del diritto.

2. La Direttiva (UE) 2016/943 e il suo recepimento nell'ordinamento italiano.

Su questo scenario solo brevemente accennato è intervenuta nel recente passato l'Unione Europea con la Direttiva 2016/943. Tale normativa mira a proteggere il *Know-how* e le informazioni commerciali riservate (segreti commerciali) avverso l'acquisizione, l'utilizzo e la divulgazione illeciti. Nonostante presenti un marcato carattere civilistico[6], la stessa costituisce, ai fini del presente lavoro, un importante tassello ricostruttivo. Essa, infatti, contiene una definizione di segreto commerciale con la quale anche il penalista deve necessariamente confrontarsi, ancor di più se si considera che il legislatore italiano ha provveduto alla modifica dell'ormai secolare disciplina penalistica in materia (art. 623 c.p.) proprio in sede di recepimento dell'atto normativo in commento.

La Direttiva (UE) 2016/943 rappresenta il primo modello di integrazione europea in materia di veri e propri segreti commerciali. Essa si fonda sull'idea secondo la quale le imprese riconoscono alle informazioni commerciali riservate lo stesso valore dei brevetti e delle altre forme di proprietà industriale. Le due forme di tutela, infatti, assolvono a funzioni tra loro diverse e spesso si pongono in rapporto di complementarietà. Anche laddove però si presentino come l'una alternativa all'altra, la centralità della riservatezza di determinate informazioni aziendali costituisce tratto distintivo dell'odierno contesto economico, tale da non poter fare più dubitare dell'opportunità di un intervento normativo in materia. Con il dichiarato intento di colmare un *gap* normativo notevole con le altre economie occidentali, *in primis* gli Stati

[4] Tra i vari e numerosi documenti che ormai utilizzano questo concetto, si rimanda all'*impact assessment* che ha accompagnato la proposta di Direttiva sulla tutela del Know-how e del segreto commerciale; disponibile al seguente link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2013:0471:FIN.

[5] *Ivi,* p. 69-70.

[6] Indice del carattere civile della Direttiva (UE) 2016/943 è costituito dalla produzione dottrinale italiana, pre e post recepimento, sul punto, rappresentata da contributi di natura (quasi) esclusivamente civilistica. Cfr. Chiabotto e Venturello (2016), p. 775 – 787; Falce (2018), p. 155 – 159; Falce (2017), p. 560 -565; Falce (2016), p. 129-139; Serafini (2018), p. 1329 – 1338; Galli *et al.* (2018).

Uniti d'America, la regolamentazione europea pone quindi standard minimi di tutela del segreto commerciale in un contesto continentale estremamente diviso, all'interno del quale non solo sono presenti definizioni di segreto in materia economica tra loro profondamente diverse, ma spesso manca del tutto una normativa specifica sull'argomento.

Ai fini della presente indagine interessa soffermarsi sulla definizione di segreto commerciale fornita dal legislatore europeo, secondo la quale sono informazioni commerciali riservate quelle che *non sono, nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, generalmente note o facilmente accessibili a persone che normalmente si occupano del tipo di informazioni in questione;* che *hanno valore commerciale in quanto segrete;* e che *sono state sottoposte a misure ragionevoli a mantenerle segrete*[7]. La definizione in commento, per quanto costituente una novità nel panorama normativo europeo, non rappresenta però un'assoluta innovazione nel contesto internazionale. Essa, infatti, riprende la definizione dell'art. 39 dei TRIPs[8] che si fondava già sulla tripartizione concettuale del segreto commerciale in riservatezza, valore intrinseco e sottoposizione a misure di protezione. Proprio per tale ragione, la definizione di cui all'art. 2 della Direttiva agli occhi del giurista italiano non costituisce fonte di particolare novità. Il nostro ordinamento infatti conosce già dal dicembre 1994 una nozione di informazione commerciale strutturata secondo le linee tratteggiate dal contesto sovranazionale, definizione confluita nel 2005 nell'art. 98 del codice della proprietà industriale, oggetto di modifiche solo marginali a seguito del recepimento della disciplina europea[9].

Dall'entrata in vigore dei TRIPs e sino al maggio 2018, quindi, l'ordinamento italiano presentava in materia di tutela del segreto nel campo economico-tecnologico una duplice anima: se il sistema penale rimaneva ancorato ad una fattispecie di stampo prettamente napoleonico, incentrata sul segreto di fabbrica e sull'idea dell'applicazione industriale, l'ordinamento civile si apriva ad una visione moderna ed anglosassone del sapere tecnologico, che poneva al centro della propria azione di tutela l'informazione commerciale in quanto tale[10].

Il contesto risulta invece profondamente mutato a seguito del recepimento della Direttiva (UE) 2016/943, con il quale il legislatore italiano pare aver abbandonato il doppio schema di tutela in favore di un modello unitario. Il D. Lgs. n. 63/2018 è infatti intervenuto con decisione sulla norma penalistica di riferimento[11], abbandonando l'impronta napoleonica dell'art. 623 c.p. in favore di una nuova ottica di tutela. La novella è intervenuta con vigore, come si mostrerà a breve, sia in merito all'oggetto di tutela sia in relazione alle modalità di aggressione al bene protetto, realizzando un totale accostamento tra la tutela civilistica e quella penalistica. Ciò spinge inevitabilmente l'interprete ad interrogarsi su due questioni parzialmente diverse ma profondamente connesse: una riguarda la reale portata di tale accostamento; l'altra l'estensione della nozione di segreto commerciale dal campo civile a quello penale. Prima però di affrontare le problematiche citate, risulta opportuno ricostruire, seppur brevemente, la disciplina penale sulla quale sono intervenute le modifiche summenzionate.

[7] Articolo 2 della Direttiva.

[8] *Trade Related Aspects of Intellectual Property Rights*, siglato a Marrakesh il 15 aprile 1994 e ratificato dall'Italia il 29 dicembre 1994.

[9] Il testo originario dell'art. 98 c.p.i. recitava "*Costituiscono oggetto di tutela le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni:*
a) siano segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore;
b) abbiano valore economico in quanto segrete;
c) siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete."
Il testo vigente, frutto delle modifiche del D.Lgs. n. 63/2018, statuisce che "*Costituiscono oggetto di tutela i segreti commerciali. Per segreti commerciali si intendono le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni:*
a) siano segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore;
b) abbiano valore economico in quanto segrete;
c) siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete."

[10] Sul punto si rimanda all'interessante ricostruzione di Giavazzi (2012), p. 49-64.

[11] Il Decreto Legislativo in questione non si è limitato a modificare l'art. 623 del c.p. Oltre ad aver apportato profonde modifiche al c.p.i., lo stesso Decreto ha parzialmente modificato altresì la disciplina dettata in materia di mancata esecuzione dolosa di un provvedimento del giudice (art. 388 c.p.). Ai fini della presente indagine ci si concentrerà però esclusivamente sulle modifiche apportate alla Divulgazione di segreti scientifici e commerciali.

3. L'art. 623 c.p. *ante* riforma e la nuova conformazione della fattispecie astratta.

La normativa penale mirante a tutelare il segreto in ambito economico costituisce il frutto diretto delle disposizioni napoleoniche a tutela del *secret de fabrication*[12]. L'art. 623 c.p. è giunto, sino al Maggio 2018, inalterato nella propria struttura e conformazione, pur essendo pervenuto nel codice Rocco senza alcuna modifica di rilievo rispetto alla codificazione precedente. L'antecedente storico dell'art. 623 c.p., l'art. 298 del codice Zanardelli[13], presentava, infatti, le medesime caratteristiche della disposizione di "Rivelazione di segreti scientifici o industriali" dell'originario testo del codice Rocco[14]. Essa si contraddistingueva per essere un reato proprio e per individuare l'oggetto del segreto nelle notizie sopra *invenzioni o scoperte scientifiche o applicazioni industriali*.

Di fronte ad un immobilismo legislativo di tal sorta[15], le esigenze della prassi economica non sono del tutto rimaste inascoltate, trovando riscontro nell'attenta opera ricostruttiva della dottrina e nella, pur scarna, applicazione giurisprudenziale. Le due maggiori difficoltà che la normativa scontava in relazione al mutare del contesto economico si concretizzavano nelle due peculiari caratteristiche sopra accennate: la ristretta cerchia di soggetti attivi del reato e l'oggetto giuridico tutelato.

In relazione alla natura di reato proprio, ad onta del tenore letterale dell'articolo, si è infatti assistito ad una progressiva estensione dei potenziali soggetti attivi. Abbandonata l'elencazione casistica delle figure di lavoratori possibili autori del reato, tipica della matrice napoleonica[16], ci si è nel corso degli anni allontanati dalle posizioni dottrinarie tendenti a riconoscere l'art. 623 c.p. come espressione penalistica dell'obbligo di fedeltà del lavoratore di cui all'art. 2105 c.c.; impostazione che limitava fortemente la cerchia di possibili soggetti attivi, individuandoli nei soli titolari del rapporto di lavoro subordinato[17]. Tale idea, figlia dell'opinione ottocentesca secondo la quale è il lavoratore il principale (se non l'unico) strumento di diffusione dei segreti dell'impresa, ha però ceduto il passo ad una più moderna interpretazione che, ricostruita la disposizione civilistica alla stregua di "*un'enfatica affermazione ideologica*" priva di "*pregnanti risvolti pratici*"[18], ha individuato tra le due norme due piani di tutela nettamente distinti, concludendo per l'impossibilità di utilizzare l'art. 2105 c.c. per la delimitazione dei soggetti attivi del reato[19] di rivelazione di segreto industriale.

Si è quindi optato per una relazione di tipo funzionale del soggetto agente con il segreto che, in conformità con le nuove esigenze del sistema economico, permetta l'estensione della cerchia di soggetti rientranti nell'ambito di operatività della norma in commento, colpendo non soltanto i lavoratori dipendenti ma altresì soggetti esterni all'ente che abbiano partecipato a vario titolo alle attività produttive dell'impresa[20]. Nonostante gli sforzi interpretativi, permaneva però, sino alla riforma del 2018, il notevole vincolo della natura di reato proprio che, anche accogliendo le tesi più estensive in materia di interpretazione della norma, non permet-

[12] Sul punto, oltre ai già citati Mazzacuva (1979) e Alessandri (1984), anche Picotti (1989), p. 1 s.

[13] L'art. 298 del codice Zanardelli prevedeva "*Chiunque rivela notizie concernenti scoperte o invenzioni scientifiche o applicazioni industriali, delle quali sia venuto a cognizione per ragioni del suo stato od ufficio o della sua professione od arte, e che dovevano rimanere segrete è punito*[..]".

[14] Così il testo precedente alla riforma del 2018 "*Chiunque, venuto a cognizione per ragioni del suo stato o ufficio, o della sua professione o arte, di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche, o applicazioni industriali, le rivela o le impiega a proprio o altrui profitto, è punito* [..]".

[15] Le uniche novità introdotte dalla nuova codificazione vertevano sull'incriminazione dell'autonoma condotta di impiego, oltre alla semplice rivelazione, e sull'utilizzo a proprio o altrui profitto. Su tale ultimo profilo, oggetto di specifico dibattito in dottrina circa la sua qualificazione alla stregua di dolo specifico [Crespi (1952), p. 285] o di evento del reato [Mazzacuva (1979), p. 121] o ancora di elemento oggettivo della condotta capace di arrecare vantaggio all'agente [Alessandri (1984), p. 269], si tornerà successivamente.

[16] Sul punto Picotti (1989), p. 8.

[17] Cfr. Crespi (1952), p. 197 s.; Mazzacuva (1979), p. 160 s.; Siniscalco (1964) p. 156 s.

[18] Alessandri (1984), p. 203.

[19] "*È al contrario apprezzabile il risultato che, sul piano sistematico, si può raggiungere staccando nettamente le due figure, osservando come esse individuino due piani di tutela di ampiezza e spessore diverso, tra loro in possibile complementarietà. In breve, durante la vigenza del rapporto di lavoro la pretesa di riservatezza è oggettivamente più intensa ed elevate, potendo abbracciare dati che non rientrerebbero nel segreto industriale. Estinto il vincolo contrattuale, il lavoratore riprende pienamente la propria libertà di iniziativa […] In conclusione, è quindi preferibile la tesi […] che non vi sia affatto coincidenza, neppure approssimativa, tra il divieto di rivelazione e di impiego ex art. 2105 c.c. e la figura di reato di cui all'art. 623 c.p., né tantomeno che quest'ultimo funga da ulteriore sanzione repressiva alla violazione dell'obbligo di fedeltà come delineato dalla seconda parte della norma civilistica. Dalla riconosciuta peculiarità dei presupposti dell'art. 2015 c.c. e della sua estensione oggettiva consegue l'impossibilità di ricavare decisivi argomenti per la selettiva individuazione dei soggetti attivi del reato tra i soli lavorati dipendenti.*" Alessandri (1984), p. 203-204. Di medesimo tenore, più di recente: Giavazzi (2012), p. 78-90.

[20] Sul punto, oltre alla dottrina riportata alla nota precedente, si rimanda a Picotti (1989), p. 10, Manno (2016), p. 566-567.

teva di rispondere alla moderne esigenze di tutela dell'impresa, la quale, in un mondo sempre più interconnesso e caratterizzato dalla presenza di beni immateriali ad altissima volatilità, è soggetta ad un sempre maggiore rischio di spionaggio economico esogeno rispetto all'ambito industriale/produttivo.

Ma l'avanzare tecnologico non rendeva la norma in commento obsoleta solo in relazione ai possibili soggetti dell'illecito. Essa infatti mostrava le proprie carenze anche, e forse soprattutto, in merito all'oggetto del segreto tutelato. Pur facendo propria una nozione di *applicazione industriale* ritenuta da unanime dottrina di ampiezza maggiore rispetto all'originario segreto di fabbrica, il testo precedente alla riforma si caratterizzava per un legame peculiare con un contesto economico prettamente industriale, in cui il segreto tutelabile doveva necessariamente estrinsecarsi in una notizia suscettibile di potenziale applicazione tecnica.

Anche laddove infatti si fosse accolta una nozione di segreto industriale in senso lato, così come sostenuto dalla giurisprudenza più recente[21], allargando l'operatività della norma sino ad includervi la nozione di *Know-how* in senso tecnico[22], il tenore letterale della disposizione non permetteva all'interprete, senza sfociare in un'operazione analogica, di sanzionare con lo strumento penale le condotte di violazione dei c.d. segreti commerciali, ed in generale di tutte quelle informazioni e dati assolutamente centrali nell'odierna *data-driven economy*[23]. La violazione del segreto commerciale non era comunque del tutto irrilevante per il sistema penale, potendo la stessa ricadere, secondo autorevole dottrina[24], nell'ambito di applicazione dell'art. 622 c.p.[25] Ciò nonostante, i ristetti margini di operatività sorti in merito alla violazione di segreto industriale si ripresentavano, con maggior vigore, in relazione alla più generale ipotesi di rivelazione di segreto professionale, comportando il sorgere dei medesimi dubbi in precedenza segnalati.

L'anacronismo della previgente disposizione di cui all'art. 623 c.p., e la sua conseguente incapacità di rispondere alle nuove esigenze poste dal processo economico, era connaturato alla conformazione stessa della fattispecie, i cui insuperabili limiti strutturali non consentivano alla scienza giuridica di procedere oltre "nell'adattamento" della norma al contesto sociale di riferimento per il tramite del delicato quanto cruciale momento interpretativo[26], rendendosi quindi opportuno un intervento legislativo. Forse perché conscio di tale necessità, il Parlamento italiano ha scelto, in sede di recepimento della Direttiva (UE) 2016/943, di intervenire anche in sede penalistica, procedendo ad una profonda riscrittura della norma, a prima vista finalizzata a soddisfare le esigenze sorte nella prassi.

L'intervento è stato particolarmente incisivo[27]. Da una parte, infatti, si è intervenuti massicciamente sull'oggetto del segreto, sostituendo, al primo comma, alla formula *applicazioni industriali* l'espressione *segreti commerciali*, uniformando la terminologia a quanto previsto dal c.p.i. Dall'altra, si è inserito un nuovo comma all'art. 623 c.p. e si è strutturato l'illecito di violazione di un segreto commerciale alla stregua di un reato comune, lasciando però la conformazione di reato proprio per le notizie sopra invenzioni o scoperte scientifiche.

Nonostante la novella ponga spunti di riflessione sotto molteplici aspetti, ai fini del presente lavoro si concentrerà l'attenzione solo sull'introduzione del secondo comma dell'art. 623 c.p. Esso recita che *la stessa pena* [reclusione sino a due anni] *si applica a chiunque, avendo acquisito in modo abusivo segreti commerciali, li rivela o li impiega a proprio o altrui profitto*. La scarna descrizione della fattispecie richiama alla mente la struttura dell'illecito civile di cui al primo

[21] Cass., Sez. V, 18 Maggio 2001, *CED* 219471, secondo la quale il segreto industriale *comprende quell'insieme di conoscenze riservate e di particolari modus operandi in grado di garantire la riduzione al minimo degli errori di progettazione e realizzazione e dunque la compressione dei tempi di produzione*.

[22] Sul punto si rimanda alla precisa ed approfondita ricostruzione di Giavazzi (2012), p. 205-252 e dottrina *ivi* richiamata.

[23] Interessante notare come, con una lungimiranza sicuramente non comune, già in sede di lavori preparatori per l'emanazione del codice penale fosse sorta l'esigenza, poi non confluita nel testo di legge approvato, di tutelare i c.d. segreti commerciali per la loro centralità già nel processo produttivo del tempo. Sul punto *Lavori preparatori del codice penale e del codice di procedura penale*, Vol. IV, p. 130-131.

[24] Per tutti Cfr. Crespi (1966), p. 184 s.

[25] L'art. 622 c.p., rubricato Rivelazione di segreto professionale, sanziona la condotta di "*Chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto può derivare nocumento* […]".

[26] La centralità del momento storico dell'interpretazione giuridica è chiaramente resa da Pagliaro (2003), p. 223 "*La norma giuridica ha una sua vita propria, intimamente connessa con quella delle altre norme giuridiche e con gli interessi e convinzioni etico-politico-religiose della società che è chiamata a disciplinare. Attraverso il meccanismo dell'interpretazione e dell'applicazione di una legge il contenuto di una norma penale può variare secondo le esigenze della società. Di conseguenza, varia l'ambito dei fatti previsti come reato. Questi profili contenutistici non devono essere dimenticati, quando si accoglie la definizione "formale" del reato*".

[27] Per un primo commento al Decreto attuativo si rimanda a Mainini (2018), p. 163-175.

comma dell'art. 99 c.p.i.[28], i cui elementi essenziali sono quasi tutti presenti nella disposizione penalistica, facendo sorgere quindi all'interprete dubbi circa la corretta definizione dei ruoli dei vari strumenti di tutela in materia di segreto commerciale.

A seguito della riforma del 2018, infatti, la sovrapposizione dei piani di tutela appare assai evidente. Entrambe le disposizioni si rivolgono ad una platea potenzialmente indiscriminata di autori, entrambe richiamano l'abusività della condotta del soggetto agente e tutti e due gli ambiti sembrano guardare alla medesima oggettività giuridica, ossia il segreto commerciale. Se, quindi, la nuova normativa sembra avere il pregio di rispondere alle necessità ed esigenze che contraddistinguono l'attuale assetto socio-economico, la stessa pone al giurista interrogativi circa una corretta suddivisione e gradazione della responsabilità del singolo, dubbi con i quali ora non ci si può esimere dal confrontarsi.

4. L'intersecarsi dei diversi piani di tutela. Differenziazione o sovrapposizione?

Come già accennato, a seguito della novella del 2018 l'ordinamento italiano ha adottato un modello unitario di tutela per i segreti in campo economico, avendo abbandonato l'impostazione tradizionale del codice penale in favore del modello civilistico di stampo anglosassone. Gli illeciti di cui agli artt. 623 c.p. e 99 c.p.i. presentano, come conseguenza di tale uniformazione, una struttura particolarmente sovrapponibile.

In primo luogo, sia la fattispecie penale sia quella contenuta nel codice della proprietà industriale si riferiscono ad una platea indiscriminata di soggetti attivi. In aggiunta, notevoli similarità sono presenti altresì con riferimento alle condotte illecite sanzionate. In entrambe, infatti, è prevista la clausola di illiceità espressa del metodo abusivo che contraddistingue le condotte, anche se con un'ampiezza parzialmente diversa. Mentre nell'illecito civile l'abusività è riferita a tutte e tre le condotte sanzionate (*acquisizione, rivelazione* e *utilizzo*), nella fattispecie penale essa si riferisce alla sola acquisizione, delineata alla stregua di un vero e proprio presupposto della condotta illecita. Se differenze possono essere rinvenute nel diverso atteggiarsi dell'elemento psicologico (solo il dolo per la fattispecie ex art. 623 c.p.) e nell'impiego a proprio o altrui profitto (sussistente solo per l'illecito penale), le due norme sembrano invece rivolgersi alla medesima oggettività giuridica: il segreto commerciale.

Una prima questione che sorge dal confronto tra le due tutele è quindi quella relativa all'ambito applicativo della nozione di segreto commerciale delineata dal codice della proprietà industriale. Di fronte, infatti, al silenzio del legislatore penalistico è lecito interrogarsi se la più che dettagliata soluzione definitoria adottata dal c.p.i. possa essere trasposta nell'ordinamento penale. La nozione di segreto commerciale cui rimanda l'art. 623 c.p. sarebbe in tal caso presa in prestito dalla normativa civilistica. Nell'ipotesi in commento, la fattispecie penale impiegherebbe un c.d. elemento normativo[29] e, di conseguenza, denoterebbe la classe di fatti attraverso l'applicabilità alla stessa di una qualifica giuridica[30].

Se si conclude per la natura di elemento normativo giuridico del concetto di segreto commerciale, che non necessita della mediazione interpretativa del giudice[31], si dovrà inevitabilmente convenire per la quasi totale sovrapponibilità delle due diverse sfere di tutela. Tale conclusione spinge l'interprete ad interrogarsi circa l'opportunità di una siffatta scelta di politica legislativa che potrebbe risultare, oltre che inefficace o inefficiente, altresì contraria ai principi regolatori la materia penale

[28] "*Ferma la disciplina della concorrenza sleale, il legittimo detentore dei segreti commerciali di cui all'articolo 98, ha il diritto di vietare ai terzi, salvo proprio consenso, di acquisire, rivelare a terzi od utilizzare, in modo abusivo, tali segreti, salvo il caso in cui essi siano stati conseguiti in modo indipendente dal terzo.*".

[29] Sul concetto di elementi normativi si rimanda alla manualistica contemporanea. Si richiama a titolo esemplificativo: Mantovani (2017) p. 63 s.; Marinucci, Dolcini e Gatta (2018) p. 63 s.; Fiandaca e Musco (2014) p. 90 s.

[30] Pagliaro (2003), p. 55.

[31] La dottrina che più di recente si è occupata dell'argomento, ha differenziato le varie categorie di elemento normativo a seconda del proprio canone di sufficiente determinatezza, e le ha distinte sulla base della loro maggiore o minore valutatività, ovvero della loro maggiore o minore attitudine ad acquisire consistenza solo per il tramite dell'interprete. Sulla base di tale criterio si sono differenziati gli elementi in questione in rigidi, elastici e vaghi. Nei primi si sono ricompresi sia gli elementi descrittivi naturalistici sia gli elementi normativi giuridici, poiché in entrambi il significato può essere compreso con immediatezza indipendentemente dalla *ratio legis* della disposizione in cui siano concretamente contenuti. Risicato (2004), p. 204.

4.1. *Il sistema civilistico punitivo di tutela del segreto commerciale.*

Il problematico coordinamento tra la tutela penale e quella civile risulta questione non particolarmente frequente nella discussione giuridica. Di norma, difficoltà di tal sorta sorgono in relazione all'altro ramo del diritto pubblico sanzionatorio: l'illecito amministrativo. È infatti in merito ad esso che la dottrina e la giurisprudenza, specialmente negli ultimi anni, si sono interrogate circa un efficace collegamento con lo strumento penalistico. Ciò nonostante, a parere di chi scrive, la tematica dei rapporti tra l'illecito civile e la tutela penale rappresenta, specie in seguito ai recenti arresti giurisprudenziali[32], un tema in costante evoluzione, e proprio per tale ragione meriterebbe un maggior dialogo tra le diverse dottrine. A riprova di ciò, le perplessità che di solito contraddistinguono il non semplice rapporto tra illecito penale e amministrativo, si ritrovano altresì nella disciplina civilistica oggetto di analisi, che si denota per sanzioni classificabili alla stregua di vere e proprie pene private, dotate di una carica afflittiva tale da far dubitare della loro reale natura.

La particolare portata della tutela civilistica è dovuta innanzitutto alla qualificazione dello stesso diritto al segreto commerciale che, a seguito della trasposizione della relativa disciplina nel c.p.i., viene classificato come un diritto di proprietà industriale autonomo e non titolato[33]. Tale qualificazione comporta inevitabilmente effetti sulla protezione assicurata al segreto che, nonostante non possa essere parificata ad una tutela *erga omnes* di stampo proprietario, è comunque dotata di un notevole raggio d'azione, sia a livello cautelare sia definitivo. Non si considera questa la sede opportuna per procedere ad una compiuta analisi del sistema civile di tutela del segreto commerciale, analisi per la quale non si ritiene financo possedere le necessarie competenze; le brevi note che seguono, che si concentreranno solo sui rimedi definitivi con particolare riguardo alla tutela risarcitoria, hanno quindi l'unico scopo di delineare i tratti salienti di una disciplina legata a doppio filo con la disposizione penalistica.

La normativa, italiana ed europea, individua tra le misure definitive strumenti dal carattere correttivo e inibitorio[34]. Tra i poteri del giudice vi è la possibilità di ordinare la cessazione di utilizzare il segreto commerciale ottenuto illecitamente, oltre all'inibizione di qualsiasi atto di immissione nel mercato di merci realizzate a seguito di violazione di segreto commerciale[35]. Ma di maggiore interesse per l'attuale indagine risulta essere la conformazione del rimedio risarcitorio, strutturato sulla falsariga dei c.d. *danni punitivi*. Di norma la linea di demarcazione tra l'illecito aquiliano ex art. 2043 c.c. e la responsabilità penale è individuata nella differente finalità perseguita che, in sede di responsabilità extracontrattuale, mira alla sola reintegrazione dei singoli diritti lesi, al fine della ricomposizione degli interessi coinvolti[36]. La classica natura della responsabilità aquiliana si discosta dalla risposta sanzionatoria penale la quale, dotata di un peculiare carattere di afflittività, mira invece alla prevenzione generale e speciale di determinate condotte ritenute lesive di interessi pubblici particolarmente rilevanti.

Vi sono però ipotesi in cui la responsabilità civile non persegue il solo fine di ricomposizione degli interessi coinvolti, ma si pone come vero e proprio deterrente di determinate condotte con una funzione quindi anche preventiva. Tra queste vi si può fare rientrare la disciplina risarcitoria stabilita dal codice della proprietà industriale ed applicabile anche al segreto commerciale[37]. Il meccanismo previsto dall'art. 125 c.p.i.[38], denominato di retroversione degli utili, in piena ottica di deterrenza impone la retroversione di qualsiasi utile generato grazie alla contraffazione, e prevede espressamente un risarcimento del danno che possa andare al di là

[32] Si fa riferimento, in particolar modo, al recente arresto delle Sez. Unite della Corte di Cassazione in merito alla compatibilità tra l'istituto dei danni punitivi e il nostro sistema di responsabilità civile. Sez. Unite sent. n. 16601 del 5 Luglio 2017. Nota di Brizzolari (2017).

[33] Auteri *et al.* (2016), p. 209 s. È comunque discussa la qualifica di *full property right,* e criticata la scelta della *sedes materiae*: Cfr. Falce (2016) p. 129 s.; Vanzetti (2011) p. 95 s.

[34] Sulle forme di tutela civilistiche si rimanda, tra gli altri, a Chiabotto e Venturello (2016), p. 775 – 787; Falce (2018), p. 155 – 159; Falce (2017), p. 560 -565; Falce (2016), p. 129-139; Banterle e Blei (2017), p. 202 s.; Galli *et al.* (2018)

[35] Art. 124 c.p.i. e art. 12 Direttiva (UE) 2016/943.

[36] A titolo esemplificativo si richiama, tra l'unanime e concorde manualistica, Trabucchi (2017), p. 1219 s.

[37] Per una ricostruzione casistica delle varie ipotesi di danni punitivi presenti nell'ordinamento italiano si rimanda a Franzoni (2018), p. 289 s.; Baratella (2006).

[38] Il carattere punitivo della disposizione emerge tanto dal disposto del primo comma "*il risarcimento dovuto al danneggiato è liquidato secondo le disposizioni degli articoli 1223, 1226 e 1227 del codice civile, tenuto conto di tutti gli aspetti pertinenti, quali le conseguenze economiche negative, compreso il mancato guadagno, del titolare del diritto leso, i benefici realizzati dall'autore della violazione e, nei casi appropriati, elementi diversi da quelli economici, come il danno morale arrecato al titolare del diritto dalla violazione*" quanto dal contenuto dell'ultimo comma "*In ogni caso il titolare del diritto leso può chiedere la restituzione degli utili realizzati dall'autore della violazione, in alternativa al risarcimento del lucro cessante o nella misura in cui essi eccedono tale risarcimento*".

degli elementi economici, comprendendo altresì gli eventuali danni morali arrecati al titolare.

A differenza quindi dell'ordinario illecito extracontrattuale, il cui sistema di tutela mira a riparare la vittima dal danno subito, il danno punitivo[39] ha lo scopo di sanzionare l'autore del fatto, giustapponendo la responsabilità civile alla responsabilità penale. Tale accostamento si riscontra già a livello di descrizione della fattispecie. Se l'ordinario illecito civile non richiede alcuna forma di tipicità[40], concentrandosi appunto sul danno cagionato e non sulla condotta realizzata, le ipotesi di danni punitivi si premurano di delineare le condotte vietate, al fine di stigmatizzarne l'antigiuridicità. In conclusione, Il danno punitivo *nasce per contrastare la frode fra privati*[41], tanto che per il suo perfezionarsi è necessaria (e sufficiente) la realizzazione della sola condotta illecita, senza che *la vittima provi di aver subito una perdita patrimoniale o non patrimoniale*[42].

Di medesimo avviso la giurisprudenza di merito e di legittimità. Già dal 2011, infatti, la Suprema Corte ha riconosciuto la funzione parzialmente sanzionatoria di tale strumento della responsabilità civile[43], dando seguito ad un orientamento delle Corti di merito che, negli ultimi anni, hanno sempre più rimarcato le peculiarità di tale strumento. Con esclusivo riferimento all'ipotesi di cui all'art. 125 c.p.i., senza pretesa alcuna di esaustività, si segnala come l'applicazione giurisprudenziale della norma in commento sia prevalentemente orientata ad una sua strutturazione secondo un canone particolarmente sanzionatorio. Pur non mancando pronunce in senso contrario[44], un orientamento di merito caratterizza l'art. 125 c.p.i. di una forte carica punitiva, facendo propria, in primo luogo, una nozione di retroversione dell'utile particolarmente ampia[45], e qualificando, in aggiunta, la stessa secondo una struttura ed una funzione nettamente diversa rispetto alla canonica responsabilità da risarcimento del danno[46].

In materia di segreto commerciale, quindi, il rimedio di tutela civilistico non si struttura secondo i canoni dell'ordinaria responsabilità aquiliana, ma tende piuttosto ad una liquidazione del danno dal carattere punitivo attenta più a sanzionare il contraffattore che a riparare il soggetto leso.

La conformazione della risposta sanzionatoria di stampo civile pone di conseguenza all'interprete particolari dubbi circa la sua legittima sovrapposizione con una equivalente, almeno per ambito di estensione oggettiva, tutela penale. Gli interrogativi sono sicuramente accentuati dalle recenti tendenze legislative[47] volte a riconoscere l'alternatività di un sistema civile di tutela sanzionatorio rispetto all'apparato repressivo penale, e dall'ormai decennale giurisprudenza della Corte Europea dei Diritto dell'Uomo in materia di legalità penale. Quest'ultimo riferimento è ai c.d. criteri Engel volti ad accertare l'eventuale "frode delle etichette" e la natura penale di una determinata misura sanzionatoria[48]. Su di essi preme ora soffermarsi.

[39] Sulla tematica, oltre ai riferimento della nota 32, si rimanda a Monateri (2016), p. 831; Scalisi (2009), p. 674; Pardolesi (2007), p. 452 s.

[40] "*Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno*" art. 2043 c.c.

[41] Franzoni (2018), p. 293.

[42] *Ibidem*.

[43] Il riferimento è a Cass., Sez. III, 14 Aprile 2011, n. 8730, con nota di Pardolesi P., *Foro it.* 2011, p. 3068.

[44] "*La retroversione degli utili del contraffattore sancita dall'art. 125, comma 3 c.p.i., deve essere intesa come voce di risarcimento dei danni per lucro cessante predeterminata dal legislatore in base ad una presunzione normativa di corrispondenza tra i guadagni perduti da un concorrente e gli utili acquisiti dall'altro, presunzione soggetta a prova contraria caso per caso, e non può invece essere interpretata né come sanzione per il contraffattore, avendo nel nostro sistema il danno risarcibile natura meramente compensativa e non punitiva, né come indennizzo da arricchimento senza causa per il contraffattore, stante la natura residuale di tale misura*" (Tribunale Roma, 30/03/2012 - Giurisprudenza annotata di diritto industriale 2013, 1, 463).

[45] Secondo la quale a tal fine "*occorre fare riferimento al c.d. margine operativo lordo, cioè al reddito dell'azienda basato solo sulla sua gestione caratteristica, al lordo di interessi, tasse, deprezzamento dei beni e ammortamenti*" (Tribunale Catania 22/07/2014 - Giurisprudenza annotata di diritto industriale 2016, 1, 1118).

[46] Sul punto "*Le misure di risarcimento dei danni e della retroversione degli utili vanno considerate distinte essendo la prima diretta a rimuovere il pregiudizio che si è verificato al patrimonio del titolare del diritto leso, la seconda a rimuovere l'arricchimento illecito realizzato nel patrimonio dell'autore dell'illecito*" (Tribunale Milano, 17/03/2014 - Giurisprudenza annotata di diritto industriale 2016, 1, 921); "*La mera contraffazione del marchio non può ritenersi, di per sé e in ogni caso, produttiva di un danno risarcibile, se non nei limiti della retroversione degli utili tratti dal contraffattore, che consente, sulla base della scelta della parte danneggiata, una liquidazione del danno autonoma, ed eventualmente punitiva, per il solo profilo del lucro cessante (mentre, per il danno emergente, è sempre necessaria una dimostrazione in concreto, secondo i principi generali)*" (Tribunale Bologna, 03/06/2013 - Giurisprudenza annotata di diritto industriale 2016, 1, 416). Recente giurisprudenza ha inoltre riconosciuto la non incompatibilità tra l'art. 13 della Direttiva 48/2004/CE (c.d. Direttiva *Enforcement*, in materia di tutela della proprietà intellettuale) e il sistema di tutela previsto dall'art. 125 c.p.i. che permette di quantificare il risarcimento oltre il danno effettivamente subito, "*L'art. 125 c.p.i. non è incompatibile con l'art. 13 della Direttiva 48/2004/CE, nella parte in cui consente alla vittima della violazione di domandare la retroversione degli utili anche per la parte eccedente il danno effettivamente subito, non impedendo la normativa europea la possibilità per il legislatore nazionale di adottare limiti di tutela superiori a quelli previsti dalla direttiva, soluzione peraltro compatibile con quanto previsto dall'art. 45.2, TRIPs*" (Corte appello Milano, 13/05/2013 - Giurisprudenza annotata di diritto industriale 2016, 1, 350).

[47] Ci si riferisce ai recenti D. Lgs. n. 7 e 8 del 2016 sui quali si tornerà in seguito.

[48] La produzione sull'argomento è particolarmente imponente. Al riguardo si rimanda, tra gli altri, a Masera (2018); Donini (2018), p. 2284

4.2. *Le possibili distorsioni della sovrapposizione delle tutele. Il sistema del c.p.i. e i criteri Engel*

Tali criteri, nella loro formulazione originaria[49], sono identificabili nei tre indici della qualifica legale/nominalistica della sanzione, della gravità della stessa e della sua finalità punitiva. In presenza di uno solo di essi la sanzione, a prescindere dalla qualifica ordinamentale, deve, secondo la giurisprudenza convenzionale, considerarsi penale. Come dimostrato però da recente dottrina, l'alternatività dei vari criteri è nella giurisprudenza della Corte Edu più apparente che effettiva, con la conseguenza che il canone della gravità della sanzione diviene spesso sotto-criterio per l'identificazione della finalità punitiva della stessa[50]. Per tale ragione si concentrerà l'attenzione prevalentemente sull'ultimo degli indici richiamati.

Il c.d. canone finalistico tende a ricostruire la sanzione in chiave teleologica per indagarne l'effettiva natura sostanziale. A tal fine si ritiene necessario ricercarne la funzione afflittivo-punitiva. L'ipotesi presa in esame in questo contributo si discosta, come visto, dalla classica funzione riparatoria di stampo civilistico per abbracciarne una *latu sensu* preventiva/deterrente. Ciò non è però sufficiente per classificare la sanzione come sostanzialmente penalistica, poiché la finalità preventiva, caratterizzante altresì la funzione della pena, è spesso individuata nella giurisprudenza della Corte Edu come alternativa alla finalità punitiva.

In realtà, come messo in luce dalla dottrina, la prevenzione svolta dalla misura sanzionatoria è dalla Corte europea richiamata sia a sostegno della sua finalità punitiva sia in antitesi alla stessa[51]. Ciò per un problema essenzialmente definitorio che riconduce al medesimo termine, *prevenzione*, due concetti tra loro distinti. Secondo i giudici di Strasburgo, la finalità preventiva di tipo *generale* è caratteristica insita alla nozione di pena, e accompagna di conseguenza la funzione sanzionatoria della stessa. Contrariamente invece alla funzione preventiva *speciale* che, seppur spesso indicata in alcuni ordinamenti (come ad esempio il nostro) quale ulteriore corollario della sanzione penale, da sola non può giustificare la qualificazione penale di una determinata misura.

È innegabile che lo strumento della retroversione degli utili presenti caratteristiche non di prevenzione speciale, non avendo la funzione di neutralizzazione di un tipo di autore, ma semmai di prevenzione generale, mirando piuttosto all'attività di deterrenza di quel determinato comportamento. Ciò nonostante la mera finalità preventivo-generale non è sufficiente per riconoscere la rilevanza penale della sanzione. Deve infatti necessariamente indagarsi se l'art. 125 c.p.i. presenti, come già detto, una vera e propria natura punitiva.

Ad avviso di chi scrive, sono presenti parametri che potrebbero far dubitare l'interprete circa la reale qualificazione dello strumento della retroversione degli utili. In primo luogo, la sanzione (*rectius* l'illecito *in toto*) sembra rivolta e calibrata sulla condotta illecita posta in essere e non sul danno cagionato. In aggiunta, sembrano essere le stesse motivazioni del legislatore storico che è intervenuto sulla materia ad orientare verso una finalità propriamente punitiva. La disposizione nasce, infatti, per una piena tutela della proprietà industriale cui oggi, come visto in precedenza, è stata accostata la disciplina del segreto commerciale. In tale ottica il legislatore, presumibilmente per l'inefficacia o la desuetudine delle norme penali vigenti in materia, ha scelto di punire con uno strumento particolarmente incisivo le condotte violanti la proprietà industriale in senso lato. Ma, a prescindere dalle eventuali finalità che hanno accompagnato il legislatore nell'introduzione della norma in commento, in questa sede si intende aderire a quella posizione dottrinale che inverte i poli della questione, e che, al fine di indagare la finalità punitiva, non guarda all'intenzione del legislatore, ma semmai alla posizione del destinatario della sanzione, spesso ignaro degli scopi della misura e consapevole esclusivamente della sofferenza che gli viene inflitta. In tal senso, sono da considerarsi misure punitive quelle che il destinatario percepisce come tali, e *che gli vengono applicate in conseguenza della commissione di un fatto illecito, e non consistono nel mero ristoro del danno cagionato*[52]. Nell'in-

s.; Mazzacuva (2017); Manes (2017) p. 988 s.; Viganò (2017); Pulitanò (2015), p. 46 s.

[49] I criteri in questione sono stati ulteriormente specificati dalla giurisprudenza successiva, che ha tentato di individuare altri parametri per poter guidare l'attività dell'interprete. Sulla successiva specificazione dei criteri Engel (i c.d. criteri Engel e dintorni) e sulla loro applicazione al caso concreto dell'espulsione amministrativa dello straniero si rimanda a Siracusa (2019), p. 109 s.

[50] Masera (2018), p. 80 s.

[51] *Ivi*, p. 71.

[52] *Ivi*, p. 214. L'autore prosegue indicando l'essenza del carattere punitivo della misura quale *un male che deriva da un comportamento illecito*, e che possiede *un contenuto afflittivo ulteriore rispetto al male arrecato*.

dagare quindi la finalità punitiva di una misura non si può prescindere dalle conseguenze che scaturiscono per il soggetto agente, e quindi dal male subito dallo stesso. In presenza di una risposta sanzionatoria che si limita al risarcimento del danno *o al rispristino della situazione ante factum*[53], non si potrà sostenere la natura punitiva della sanzione.

Tentando di applicare i principi ora individuati al caso di cui ci si occupa, sembra non potersi escludere a priori la natura punitiva del sistema rimediale civile previsto per la violazione di un segreto commerciale. Esso, infatti, è del tutto sganciato dal danno arrecato al titolare del segreto e fa propria una nozione di utile, fondata sul *margine operativo lordo*, che sembra andare al di là del mero ripristino della situazione *ante factum*. Se è da ritenersi vero che lo scopo riparatorio esclude la natura punitiva della sanzione, è però altrettanto corretto affermare che dalla mancata funzione di ripristino non può desumersi automaticamente l'afflittività tipica delle sanzioni penali. Al riguardo, dubbi circa tale qualificazione sostanziale sorgono laddove si decida di procedere nell'analisi per mezzo dell'utilizzo degli ulteriori criteri (e sotto-criteri) individuati dalla giurisprudenza convenzionale.

In primo luogo, si potrebbe negare il carattere della particolare gravità della sanzione che, pur essendo un criterio parzialmente subalterno al canone funzionalistico, viene spesso utilizzato dalla Corte Edu per la risoluzione dei casi irrisolti alla luce della chiave teleologica[54]. Pur potendo sussistere la gravità della misura anche in presenza di sanzioni che non incidano sulla libertà personale del sottoposto, si potrebbe nel caso di specie dubitare della particolare afflittività della sanzione posta in essere ex art. 125 c.p.i. Anche l'ulteriore sotto-criterio del collegamento con il procedimento penale sembra nel caso di specie del tutto assente, non essendo la sanzione emessa da un giudice penale e non sussistendo nessuna forma di collegamento tra la sanzione e la responsabilità penale. Dell'utilità di tale sotto-criterio si potrebbe però dubitare alla luce della recente depenalizzazione, che ha sancito la creazione di un vero e proprio sistema civile di tipo sanzionatorio sganciato del procedimento penale. La normativa in questione, diretta attuazione del principio di *extrema ratio* della sanzione criminale, costituisce espressione del principio di sussidiarietà del diritto penale e spinge ad un ripensamento dei normali rapporti tra quest'ultima branca del diritto e l'ordinamento civile. Tale mutamento di paradigma non può ora non essere preso in considerazione, poiché riconosce altresì allo strumento civile, laddove dotato di peculiari caratteristiche, la funzione di orientamento delle condotte dei consociati, e quindi può costituire ulteriore stella polare per l'individuazione dei criteri utili per discernere i classici rimedi civili dalle sanzioni pecuniarie aventi carattere punitivo.

4.3. *I nuovi rapporti tra la tutela civile e la sanzione penale*

L'idea del diritto penale come *ultima ratio* dell'ordinamento[55] agita la scienza giuridica da decenni, e ha trovato di recente un deciso sbocco applicativo. Ci si riferisce alla legge delega n. 67 del 2014, successivamente confluita nei D. Lgs. n. 7 e 8 del 2016[56]. La disciplina, frutto di quattro diverse deleghe conferite al Governo, si pone nell'ottica di assicurare alla sanzione penale la natura sua propria di intervento puntiforme ed eccezionale del sistema pubblico di protezione degli interessi rilevanti. La necessità di arretramento del diritto penale, incentrato ancor oggi sull'invasiva pena detentiva, è particolarmente sentita in un sistema democratico strutturato intorno alle libertà del singolo, che dovrebbe consentire il sacrificio della libertà personale del cittadino solo in presenza di determinate aggressioni, secondo una rigida scala di graduabilità dell'intervento pubblico che tenga in debita considerazione tutti i possibili strumenti giuridici di orientamento delle condotte dei consociati.

Proprio in ottica di ampliamento delle tecniche di controllo sociale si pone il D. Lgs. n. 7/2016, che si caratterizza per l'elevato grado di innovatività rispetto alle più consuete tecniche di depenalizzazione. All'abrogazione di talune fattispecie delittuose, espressive di interessi c.d. minori[57], non ha fatto seguito l'introduzione di illeciti amministrativi, secondo l'opzione

[53] *Ibidem.*
[54] *Ivi*, p. 88.
[55] Oltre all'imponente produzione manualistica sull'argomento si rimanda, tra gli altri, a Marra (2018); Gargani (2018), p. 1488 s.; Paliero (2018), p. 1447 s.; Demuro (2013) p. 1654 s.; Bricola (1984), p. 20 s.
[56] Al riguardo, su tutti, Palazzo (2014), p. 1700 s.
[57] I reati oggetto di abrogazione integrale, ai sensi dell'art. 1 del Decreto, sono: 485 (*Falsità in scrittura privata*), 486 (*Falsità in foglio firmato*

politico-criminale di carattere tradizionale[58], ma piuttosto la previsione di specifiche sanzioni pecuniarie civili, strutturate alla stregua di vere e proprie pene private[59]. Il sistema delineato dal legislatore delegato si presenta infatti come un vero e proprio *tertium genus* di tutela, all'interno del quale alla classica funzione riparativa della sanzione civile si accosta (o meglio, si sostituisce) una finalità punitiva. La natura afflittivo-punitiva del sistema ex D. Lgs. n. 7/2016 emerge dalla centralità della condotta del soggetto nel procedimento di quantificazione della sanzione e dalla rilevanza della personalità dell'agente. I criteri di commisurazione fissati dall'art. 5 del decreto rimandano infatti all'art. 133 c.p., indicando, tra gli altri, come elementi necessari per la quantificazione dell'importo della sanzione, la *gravità della violazione*, la *reiterazione dell'illecito* e la *personalità dell'agente*. La finalità preventiva è inoltre enfatizzata dalla disciplina sulla reiterazione dell'illecito di cui al successivo articolo 6, corroborata altresì dalla previsione di un apposito registro informatizzato dei provvedimenti in materia di sanzioni pecuniarie civili da tenere presso il Ministero della Giustizia (art. 11).

L'intervento legislativo in commento si pone quindi in una *prospettiva di un incremento delle alternative (civilistiche) di tutela*[60], al fine di attribuire al diritto penale il ruolo suo proprio di *extrema ratio* dell'ordinamento, e spinge l'interprete a riconsiderare, nel solco di tale innovazione legislativa, l'intero rapporto intercorrente tra le forme civilistiche di tutela e quelle più propriamente sanzionatorie[61]. In quest'ottica, il giurista non può esimersi dall'interrogarsi circa l'opportunità di sovrapporre talune peculiari tutele civili alle canoniche normative penali di protezione di beni giuridici rilevanti.

Come però già sottolineato, il carattere punitivo del sistema ex D. Lgs. n. 7/2016 emerge dalla particolare attenzione in esso posta a criteri di quantificazione della sanzione particolarmente incentrati sulla personalità del reo e sulla sua condotta precedente e successiva all'illecito, e dalla contestuale concretizzazione astratta della sanzione in ampie forbici edittali espressive di una crescente e diversificata afflittività. Tali elementi sono in realtà assenti nell'art. 125 c.p.i., e la loro mancanza costituisce importante indizio della natura sostanzialmente non penale dell'istituto della retroversione degli utili. Lo strumento di cui al codice della proprietà industriale possiede, come visto, una sicura valenza deterrente ma essa è limitata all'avvenuto illecito arricchimento, il quale può assumere una caratterizzazione a tratti punitiva ma mai, qui si crede, tale da connotarla come una vera e propria sanzione penale. Le recenti evoluzioni normative dimostrano però come l'armamentario a disposizione dell'ordinamento per l'orientamento delle condotte dei consociati sia oggi particolarmente variegato, e che in esso lo strumento penale rappresenti l'ultima (oltre che la più opprimente) arma di deterrenza. Il legislatore delegato del 2016 ha mostrato chiaramente la strada da percorrere: in presenza di illeciti espressivi di conflitti inter-privati, il diritto penale diviene un mezzo abnorme di intervento, al di là dei limiti della razionalità del sistema.

Nondimeno, le condotte di violazione del segreto commerciale non posseggono una mera valenza intersoggettiva poiché, in alcune ipotesi, possono inevitabilmente denotarsi, come si mostrerà a breve, per la finalità pubblicistica di tutela della libera concorrenza. Tuttavia, in presenza di due illeciti in materia di segreto (art. 623 c.p. e 99 c.p.i.) pressoché sovrapponibili nella loro descrizione astratta, lo sforzo per una corretta integrazione delle due norme, nel rispetto del principio di frammentarietà del diritto penale, deve essere compiuto dall'interprete, e non può che avere ad oggetto la nozione di segreto commerciale ai fini della legge penale, comportando un abbandono dell'idea del mero richiamo alla nozione civilistica. Le particolari funzioni della normativa penale hanno infatti inevitabili riflessi sia sulla conformazione del testo normativo sia sulla sua interpretazione. Come sostenuto da autorevole dottrina *il termine tecnico proprio di altra branca del diritto porta celata in sé una componente teleologica che, trapiantata inavvertitamente nel diritto penale, può generare effetti strani o comunque non desiderabili*[62]. Il trapianto di tali termini non dovrebbe quindi mai avvenire in modo acritico dovendo essere piuttosto guidato, e filtrato, dai fini peculiari della normativa penale.

La necessità di un intervento penale, seppur limitato, in materia è inoltre resa evidente dal

in bianco. Atto privato), 594 (*Ingiuria*), 627 (*Sottrazione di cose comuni*), 647 (*Sottrazione di cose smarrite, del tesoro o di cose avute per errore o caso fortuito*).

[58] Sulle peculiarità di tale processo di depenalizzazione, Cfr. Gargani (2016), p. 577 s.

[59] Sul concetto di pena privata, in riferimento alla sola letteratura penalistica, si rimanda a Bricola (1985), p. 27 s.; Padovani (1985), p. 55 s.

[60] Le potenzialità di tale scelta di politica-criminale, che considera l'opzione civilistica sia in chiave alternativa sia cumulativa all'opzione penale, erano già state colte da Bricola (1985), p. 32.

[61] Sul punto si rimanda, tra gli altri, a Piergallini (2012), p. 1299 s.

[62] Pagliaro (2009), p. 456.

sempre maggiore ricorso all'azione penale in tema di segreto commerciale. Negli anni recenti, infatti, nonostante gli invasivi mezzi civilistici contenuti nel c.p.i., l'art. 623 ha conosciuto una nuova giovinezza, costituendo ciò indice di una richiesta di tutela particolarmente sentita dai consociati. A prescindere quindi dagli efficaci strumenti di tutela ex artt. 98 e s. c.p.i., l'azione penale sembra possedere delle caratteristiche tali da renderla ancora particolarmente appetibile ai titolari dei segreti in ambito economico. Non si può infatti trascurare che, data l'inafferrabilità dei beni coinvolti e degli stessi strumenti moderni di aggressione, le difficoltà probatorie che incontra il privato in quest'ambito sono talmente notevoli da spingere verosimilmente i soggetti passivi a tentare la strada dell'azione penale per poter "sfruttare" i poteri di indagine della pubblica accusa, certamente più idonei per l'*identificazione dell'autore* e per la *ricostruzione della condotta illecita nella sua interezza*[63].

5. Osservazioni conclusive. L'art. 623 c.p. come fattispecie a tutela della libera concorrenza tra imprese.

Come si è tentato di porre in evidenza, l'intervento penale nella tematica del segreto commerciale risulta ancor oggi necessario, seppur limitato nel suo raggio d'azione. Le recenti tendenze legislative espressive di una vocazione minimizzante dello strumento penale, unite alla particolare conformazione della tutela civile nell'ambito della proprietà industriale, spingono infatti verso considerazioni che tendono a circoscrivere l'art. 623 c.p. alle sole aggressioni al bene giuridico dotate di una valenza pubblicistica e quindi di un peculiare disvalore concreto. A tal fine, risulta necessario indagare se la recente modifica della normativa penale in materia di violazione di segreto abbia influito in modo significato sul bene giuridico protetto dalla norma.

Sotto la vigenza della precedente formulazione dell'art. 623 c.p. si contendevano il campo diversi orientamenti in merito all'individuazione del bene giuridico tutelato dalla disposizione penalistica. Secondo una più risalente dottrina, il bene protetto dalla norma in commento si concretizzava nella libertà individuale di ricerca scientifica[64]. Si traeva tale soluzione basandosi prevalentemente sulla collocazione sistematica della norma che, disposta a tutela della libertà individuale, rappresentava l'egida sotto la quale poteva trovare esplicazione la libera personalità dell'imprenditore. Il ragionamento trovava inoltre sponda nel carattere marcatamente tecnico e industriale della precedente formulazione della disposizione e quindi nella sua spiccata natura scientifica. Non mancava però chi, già allora, sottolineava il carattere economico della norma in commento, individuando l'oggetto di tutela nell'esercizio indisturbato dell'attività industriale e quindi nella protezione di quelle nozioni tecniche particolarmente redditizie per l'impresa[65]. Nonostante il tenore letterale del vecchio articolo 623 c.p., parte della dottrina ha già da tempo rilevato come oggetto di tutela della disposizione siano, non le invenzioni o le notizie sopra le stesse, ma piuttosto il vantaggio concorrenziale derivante dalla loro disponibilità e del loro utilizzo.

Persa quindi la connotazione di norma a tutela dell'attività intellettiva della persona, posizione che non riusciva a spiegare il perché il segreto fosse tutelato altresì avverso il suo stesso inventore, la disposizione si contraddistingueva per tutelare una vera e propria signoria di fatto su una notizia avente caratterizzazione economica e capace di assicurare al suo titolare un vantaggio concorrenziale nel mercato di riferimento. L'impostazione in commento era però costretta a concludere, dato il tenore letterale dell'articolo, per una solo parziale natura patrimoniale dell'interesse protetto e per una non piena tutela del vantaggio concorrenziale del soggetto passivo. Quest'ultimo, infatti, non era tutelato avverso i suoi concorrenti, ma solo contro le azioni illecite poste in essere da soggetti dotati di una *privilegiata possibilità di accedere*[66] al segreto industriale. I concorrenti dell'imprenditore potevano rispondere del reato di violazione di segreto industriale solo a titolo di concorso. La tutela della libera concorrenza

[63] Giavazzi (2012), p. 516 s. che indica tra i possibili fattori di preferenza per l'area penale anche la segretezza delle indagini. Sul punto è però intervento il recente Decreto di recepimento della Direttiva (UE) 2016/943 che ha introdotto una specifica disposizione, l'art. 121 *ter* c.p.i., volto ad assicurare la riservatezza dei segreti commerciali nel corso dei procedimenti giudiziari che li hanno ad oggetto.
[64] Albamonte (1974), p.267 s.; Brignone (1980), p. 97 s.
[65] Mazzacuva (1979), p. 64 s.; Crespi (1952), p. 37 s.
[66] Picotti (1989), p. 13.

del mercato rimaneva quindi sullo sfondo dell'art. 623 c.p., la cui scena era dominata da una non meglio precisata esigenza di segreto, caratterizzata sì da un contenuto economico, ma sottoposta ad un'ingiustificata restrizione applicativa.

Il quadro sembra essere però del tutto mutato. Le pur corrette osservazioni della dottrina sopra riportate devono infatti fare i conti con il nuovo assetto della fattispecie astratta che, secondo quanto previsto dal secondo comma dell'art. 623 c.p., sanziona oggi le condotte di *chiunque rivela o impiega a proprio o altrui profitto un segreto commerciale acquisito abusivamente*.

Venuta meno la limitazione soggettiva, di cui si è dato conto in precedenza, si accentua la caratterizzazione patrimoniale della fattispecie, che viene ulteriormente enfatizzata dall'estensione dell'oggetto di tutela, oggi non più limitato alle cognizioni segrete dotate del carattere della potenziale applicazione tecnica, ma esteso piuttosto a qualsiasi informazione riservata dotata di valore per l'attività d'impresa. Fulcro della fattispecie di cui al secondo comma dell'art. 623 c.p. diviene inevitabilmente il vantaggio competitivo, realizzato non tramite i più canonici strumenti della proprietà industriale (brevetto, marchio, etc.) ma per mezzo di una vera e propria signoria di fatto su dati ed informazioni nascoste al pubblico. Prova ne è il fatto che il diretto concorrente diviene possibile, se non principale, soggetto attivo del reato.

Che l'oggetto di tutela specifico sia divenuto interamente patrimoniale, seppur nella caratterizzazione del vantaggio competitivo, lo dimostra la peculiare condotta dell'impiego a proprio profitto. Tale agire illecito, infatti, non reca con sé né la rottura di un particolare dovere di fedeltà o lo sfruttamento di una privilegiata posizione (come era sotto la previgente disposizione) né una violazione pubblica o una condivisione con terzi del segreto; esso piuttosto lede la posizione di forza dell'imprenditore nel mercato assicurata dall'esclusivo utilizzo del segreto commerciale. Da ciò inoltre deriva, ad avviso di chi scrive, che l'impiego ad altrui profitto, divenendo momento espressivo della lesività del bene giuridico tutelato, debba essere qualificato vero e proprio evento del reato in questione, e non mero atteggiamento psichico.

Se l'impostazione che si suggerisce risulta corretta, essa non può che avere effetti anche sulla nozione di segreto commerciale che si vuole accogliere in sede penalistica. Innanzitutto, una lettura della norma in chiave concorrenziale porta inevitabilmente l'interprete a propendere per una nozione di segreto in senso oggettivo[67]. Il segreto commerciale rilevante ai fini del diritto penale è quindi quello dotato di un effettivo valore economico, tutelante un interesse obiettivo dell'impresa, e non piuttosto il segreto divenuto tale per mera volontà del suo titolare. Da ciò discende, inevitabilmente, che il concetto di nocumento, sovente individuato dalla legislazione sui reati avverso il segreto ma assente nella fattispecie di cui ci si occupa, debba considerarsi un requisito implicito alla norma in esame, soprattutto per la condotta di mera rivelazione. Se già sotto la vigenza della precedente formulazione in dottrina vi era chi tacciava la norma di eccessivo *intento rigoristico*[68], la recente "apertura" concorrenziale della disposizione non può che recare con sé il necessario requisito di un pregiudizio per il detentore del vantaggio concorrenziale, e quindi di un nocumento per il titolare del segreto commerciale. Tale forma di lesione, vista la nuova oggettività giuridica della norma, non può che consistere in una perdita (o messa in pericolo) della posizione di vantaggio assunta dall'imprenditore sul mercato, con la conseguenza che il segreto commerciale tutelabile in sede penale sarebbe solo quello la cui violazione è capace di arrecare pregiudizio alla posizione dell'impresa nel mercato di riferimento.

Il segreto commerciale sarebbe quindi sottoposto a tutela nelle diverse aree dell'ordinamento, ma l'avvio della macchina penale sarebbe possibile solo in presenza delle più gravi violazioni del segreto commerciale, capaci di mettere a rischio la posizione dell'impresa nel contesto del mercato concorrenziale. In tal modo, la due forme di tutela non sarebbero tra loro sorde e non comunicanti, ma riuscirebbero ad interagire secondo un'ottica più canonica di graduabilità della responsabilità, abile a riservare al sistema penale la sua natura di ultima risposta dell'ordinamento alle condotte dei privati. Ciò è reso possibile altresì dalla particolare incisività del sistema civile italiano di protezione del segreto, il quale è tutelato alla stregua di una qualsiasi altra forma di proprietà industriale per il tramite di forme risarcitorie ai limiti dell'afflittività.

Tale chiave di lettura, che mira ad integrare i due diversi sistemi di tutela, si pone inoltre in linea di continuità con la recente riforma di depenalizzazione poc'anzi richiamata, che ha

[67] Sul punto si era già espressa autorevole dottrina: Crespi (1952) p. 43 s.; Crespi (1966) p. 283.
[68] Vigna e Dubolino (1989), p. 1094.

sottolineato l'importanza della funzione stigmatizzante del diritto penale, qui mantenuta solo per i fatti di maggiore gravità, in relazione a *fenomeni criminali che, seppur attualmente ancora di scarsa incidenza sul carico giudiziario, meritano tuttavia rilievo penale in quanto attengono a fenomeni […] in via di drammatica espansione*[69].

In conclusione, l'intervento del legislatore italiano, seppur forse in parte frettoloso, sembra, nonostante qualche chiaro-scuro, porsi in un'ottica di maggiore coerenza del sistema normativo nel suo complesso e di rispondenza dello stesso con la nuova realtà economica circostante. Peraltro, alcuni dubbi ancora permangono. Non si comprende del tutto, ad esempio, il significato del trattamento differenziato tra il segreto commerciale, oggetto di tutela a tutto tondo, e le notizie sopra invenzioni o scoperte, che sottostanno al vecchio paradigma del reato proprio. Ed ancora le sanzioni previste risultano essere non dotate di una reale efficacia dissuasiva, essendo preferibile al riguardo una loro profonda revisione. In ultimo, vista la natura di sostanziale illecito di mercato assunta dalla nuova formulazione del 623 c.p., almeno per il secondo comma, potrebbe risultare di grande utilità estendere la responsabilità amministrativa da reato degli enti anche a tale fattispecie. Ciò nonostante, ad avviso di chi scrive, se si ricostruisce un corretto rapporto di tipo integrativo tra la tutela civile e quella penale in materia di segreto commerciale, l'intervento del Parlamento, seppur tardivo e forse parziale, risulta essere un corretto e dovuto adeguamento alle moderne dinamiche dell'agire economico.

Bibliografia

Alessandri, Alberto (1984): *Riflessi penalistici della innovazione tecnologica* (Milano, Giuffrè)

Auteri, Paolo *et al.* (2016): *Diritto industriale. Proprietà intellettuale e concorrenza* (Giappichelli, Torino)

Banterle, Francesco e Blei, Marco (2017): "Alcune novità introdotte dalla Direttiva trade secret", *Rivista di diritto industriale*, p. 202 s.

Baratella, Maria Grazia (2006): *Le pene private* (Giuffrè, Milano)

Bricola, Franco (1985): "La riscoperta delle pene private nell'ottica del penalista", in Busnelli – Scalfi *Le pene private*, p. 27 s.

Bricola, Franco (1984): "Tecniche di tutela penale e tecniche alternative di tutela", in De Acutis – Palombarini *Funzioni e limiti del diritto penale*, p. 20 s.

Brizzolari, Valerio (2017): "Danni punitivi, dall'ordinamento americano a quello italiano", *GiustiziaCivile.com*, 31 Ottobre 2017

Chiabotto, Alessio e Venturello, Marco (2016): "La protezione dei segreti commerciali: la direttiva UE 2016/943", *Contratto e Impresa/Europa*, p. 775-787

Crespi, Alberto (1952): *La tutela penale del segreto* (Priulla, Palermo)

Crespi, Alberto (1966): "Tutela penale del segreto e concorrenza sleale", *La repressione penale della concorrenza sleale*, p. 181-202

Demuro, Gian Paolo (2013): "Ultima ratio: alla ricerca di limiti all'espansione del diritto penale, *Rivista italiana di diritto e procedura penale*, p. 1654-1694

Donini, Massimo (2018): "Septies in idem. Dalla materia penale alla proporzione delle pene multiple nel modelli italiano ed europeo, *Rivista italiana di diritto e procedura penale*, p. 2284 s.

[69] Relazione illustrativa allo schema di decreto legislativo n. 246 p. 8. La relazione giustifica in tal modo il mancato esercizio della delega per talune fattispecie di reato, quale ad esempio l'occupazione di luoghi privati. Le medesime ragioni sembrano rinvenibili, seppur con le dovute differenziazioni, nel settore di cui ci si occupa, oggi interessato da una sempre maggiore attività di spionaggio, anche internazionale.

Falce, Valeria (2016): "Tecniche di protezione delle informazioni riservate. Dagli accordi TRIP's alla Direttiva sul segreto industriale", *Rivista di diritto industriale*, p. 129-139

Falce, Valeria (2018): "Dati e segreti. Dalle incertezze del Regolamento *Trade secret* ai chiarimenti delle Linee Guida della Commissione UE", *Il diritto industriale*, p. 155 – 159

Falce, Valeria (2017): "Segreto commerciale, concorrenza sleale e diritto di proprietà intellettuale. Certezze e perplessità della Dir. UE 2016/943", *Il diritto industriale*, p. 560 -565

Fiandaca e Musco (2014): *Diritto penale, parte generale* (Bologna, Zanichelli)

Franzoni, Massimo (2018): "Danno punitivo e ordine pubblico", *Rivista di diritto civile*, p. 283 s

Galli, Cesare *et al.* (2018): *Il nuovo diritto del Know-how e dei segreti commerciali* (Padova, Wolter Kluver Italia)

Giavazzi, Stefania (2012): *La tutela penale del segreto industriale* (Milano, Giuffrè)

Gargani, Alberto (2018): "Il diritto penale quale extrema ratio tra post-modernità e utopia", *Rivista italiana diritto e procedura penale*, p. 1488 s.

Gargani, Alberto (2016): "La depenalizzazione bipolare: la trasformazione di reati in illeciti amministrativi sottoposti a sanzioni pecuniarie amministrative e civili", *Diritto penale e processo*, p. 577 s.

Mainini, Daniela (2018): "Le nuove regole sulla disciplina della tutela penale del segreto", *Il nuovo diritto del Know-how e dei segreti commerciali* (Padova, Wolter Kluver Italia)

Manes, Vittorio (2017): "Profili e confini dell'illecito parapenale", *Rivista italiana di diritto e procedura penale*, p. 988 s.

Manno, Marco Andrea (2016): *La tutela dell'inviolabilità dei segreti* in *Trattato di diritto penale, Vol XIV, Reati contro la persona,* Romano Bartolomeo (a cura di), p. 553-576

Mantovani, Ferrando (2017): *Diritto Penale* (Wolters Kluver Italia, Padova)

Marinucci, Dolcini e Gatta (2018): *Manuale di diritto penale* (Milano, Giuffrè)

Marra, Gabriele (2018): *Extrema ratio ed ordini sociali spontanei: Un criterio di sindacato sulle fattispecie penali eccessive* (Giappichelli, Torino)

Masera, Luca (2018): *La nozione costituzionale di materia penale* (Giappichelli, Torino)

Mazzacuva, Francesco (2017): *Le pene nascoste. Tipologia delle sanzioni punitive e modulazione dello statuto garantistico* (Giappichelli, Torino)

Mazzacuva, Nicola (1979): *La tutela penale del segreto industriale* (Milano, Giuffrè)

Monateri, Pier Giuseppe (2016): "Le delibabilità delle sentenze straniere comminatorie di danni punitivi finalmente al vaglio delle Sezioni Unite", *Danno e responsabilità*, p. 831 s.

Padovani, Tullio (1985): "Lectio brevis sulla sanzione", in Busnelli – Scalfi *Le pene private*, p. 55 s.

Pagliaro, Antonio (2003): *Principi di diritto penale* (Milano, Giuffrè)

Pagliaro, Antonio (2009): "Testo e interpretazione delle leggi penali", *Il diritto penale tra norma e società*, Vol. III

Palazzo, Francesco (1979): *Il principio di determinatezza nel diritto penale* (Milano, Giuffrè)

Palazzo, Francesco (2014): "Nel dedalo delle riforme recenti e prossime venture", *Rivista italiana diritto e procedura penale*, p. 1700 s.

Paliero, Carlo Enrico (2018): "Extrema ratio: una favola raccontata a veglia?", *Rivista italiana diritto e procedura penale*, p. 1447 s.

Pardolesi, Paolo (2007): "Danni punitivi", voce in *Digesto delle discipline privatistiche*, p. 452 s.

Picotti, Lorenzo (1989): "Invenzioni industriali (tutela penale)", *Enciclopedia giuridica Treccani*, XVII, p. 1-16

Pulitanò, Domenico (2015): "Paradossi della legalità. Fra Strasburgo, ermeneutica e riserva di legge", *Rivista trimestrale di diritto penale contemporaneo*, p. 46 s.

Risicato, Lucia (2004): *Gli elementi normativi della fattispecie penale* (Milano, Giuffrè)

Scalisi, Vincenzo (2009): "Illecito civile e responsabilità: fondamento e senso di una distinzione", *Rivista di diritto civile*, p. 658 s.

Serafini, Stefania (2018): "Luci ed ombre della nuova disciplina sul segreto commerciale", *Il corriere giuridico*, p. 1329 – 1338

Siniscalco, Marco (1964): "Rivelazione di segreti scientifici o industriali, limiti della fattispecie consumata e tentativo", *Diritto dell'Economia*, p. 155 s.

Siracusa, Licia (2018): "L'espulsione del migrante e la materia penale tra punizione e prevenzione", Militello, Vincenzo e Spena, Alessandro (a cura di), *Mobilità sicurezza e nuove frontiere tecnologiche* (Giappichelli, Torino)

Trabucchi, Giuseppe (a cura di) (2017): *Istituzioni di diritto civile* (Wolter Kluver Italia, Padova)

Vanzetti, Adriano (2011): "La tutela "corretta" delle informazioni segrete", *Rivista di diritto industriale*, p. 95 s.

Viganò, Francesco (2017): "Nullum crimen conteso: legalità costituzionale vs legalità convenzionale?", *Diritto penale contemporaneo*

Williams, Robert D. (2011): "(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action", *The George Washington Law Review*, p. 1162-1200

L'abuso di mercato nell'era delle nuove tecnologie. *Trading* algoritmico e principio di personalità dell'illecito penale

Abuso del mercado en la era de las nuevas tecnologías. Trading *algorítmico y principio de responsabilidad penal personal*

Market Abuse in the Age of New Technologies. Algorithmic Trading and Principle of Individual Criminal Responsibility

Marta Palmisano
Dottore di ricerca in Diritto Penale presso l'Università di Palermo
marta.palmisano@unipa.it

Abusi di mercato | Abuso de mercato | Market Abuse

Abstracts

L'evoluzione tecnologica ha aperto il varco, nel settore penalistico, a nuovi scenari problematici. Anche in ambito finanziario si assiste ad un mutamento delle tradizionali modalità operative, con conseguenze rilevanti nel settore dell'abuso di mercato. In particolare, la difficoltà di distinguere l'azione umana da quella dei programmi informatici è aggravata dal ricorso ai cd. algoritmi ad alta frequenza (HFT), caratterizzati dalla velocità di acquisizione ed elaborazione delle informazioni e dalla peculiare autonomia "decisionale" rispetto ad eventuali istruzioni impartite dai soggetti-persone fisiche. Il presente studio si pone pertanto l'obiettivo di verificare, anche alla luce della normativa europea, l'adeguamento delle fattispecie previste in materia di *market abuse* ai mutamenti determinati dall'innovazione tecnologica, nonché di valutare la compatibilità del sistema di negoziazione mediante HFT rispetto all'irrinunciabile principio di personalità della responsabilità penale.

La evolución tecnológica ha abierto el camino a nuevos escenarios problemáticos en el sector penal. Por otra parte, también en el sector financiero se ha producido un cambio en los métodos operativos tradicionales, con importantes consecuencias en el ámbito del abuso de mercado. La dificultad de distinguir la acción humana de la de los programas informáticos se ve agravada en particular por el uso de los algoritmos de alta frecuencia (HFT), caracterizados por la velocidad de adquisición y procesamiento de informaciones y por su peculiar "autonomía de decisión" con respecto a las instrucciones impartidas por sujetos-personas físicas. Por consiguiente, el objetivo de este estudio es verificar, también a la luz de la normativa europea, la adecuación de los casos previstos por la ley en el ámbito del abuso de mercado a los cambios causados por la innovación tecnológica, además de evaluar la compatibilidad del sistema de negociación de alta frecuencia con el principio irrenunciable de personalidad de la responsabilidad penal.

Technological evolution has opened the way for new paradigms in criminal law. A change in the traditional operating procedures has impacted finance as well, with significant consequences for market abuse. In particular, the difficulty in distinguishing human action from computer programs' is aggravated by the use of the so-called high-frequency trading (HFT), characterized by the speed of acquisition and processing of information and by "decision-making" autonomy with respect to any instructions given by natural persons. The purpose of this study is therefore to verify, in light of the European legislation as well, the adaptation of the types of offence provided by law in the field of market abuse due to technological innovation, and to assess the compatibility of the trading system through HFT with the inalienable principle of personality of criminal responsibility.

Sommario

1. Introduzione.

La forte evoluzione che ha caratterizzato il panorama internazionale, interessato dall'inarrestabile sviluppo delle nuove tecnologie, ha aperto il varco, anche nel settore penalistico, a nuovi scenari problematici. Si pensi alle interazioni tra diritto penale, scienza e nanotecnologie, al rapporto tra le emergenti intelligenze artificiali e il principio di personalità della responsabilità penale, allo sviluppo del fenomeno della criminalità informatica nell'ambito del *cyberspace*, alla tutela dei diritti umani e, in particolare, alla tutela del diritto alla riservatezza.

Nel contesto del presente lavoro si intendono tuttavia approfondire le ricadute dell'innovazione tecnologica sul piano economico, anche in ragione delle forti ripercussioni che ne conseguono in una prospettiva sovranazionale e degli interessi giuridici coinvolti, di rilevanza collettiva e internazionale.

In particolare, con riferimento al settore finanziario, l'inarrestabile progresso tecnologico ha comportato, negli ultimi anni, un radicale mutamento delle tradizionali modalità operative all'interno del mercato, determinando delle conseguenze rilevanti, sul piano penalistico, anche nel settore dell'abuso di mercato.

Invero, nel contesto finanziario, si assiste oggi ad un cambio di paradigma, per cui appare più difficile distinguere l'azione umana da quella di elaboratori e programmi informatici che investono nel mercato in modo sempre più indipendente ed autonomo rispetto alle eventuali istruzioni impartite dai soggetti-persone fisiche.

Tale situazione appare peraltro aggravata dal ricorso, sempre più frequente, a nuovi strumenti informatici, i cd. algoritmi ad alta frequenza (*High-Frequency Trading*), modalità operative caratterizzate dalla velocità di acquisizione ed elaborazione delle informazioni di mercato e di reazione a tali informazioni, nonché da una certa "autonomia decisionale".

Il presente studio, pertanto, dopo una breve disamina delle fattispecie penalistiche che vengono in rilievo in materia di *market abuse*, si pone l'obiettivo di descrivere i predetti algoritmi ad alta velocità ed esaminare le principali strategie di negoziazione adottate dagli operatori che vi facciano ricorso; tale disamina è diretta in primo luogo a verificare, anche alla luce della disciplina europea, se le fattispecie oggi esistenti tengano nella dovuta considerazione i mutamenti che l'introduzione di nuove tecnologie hanno comportato nella disciplina degli abusi di mercato e, in secondo luogo, a valutare la compatibilità del sistema di negoziazione mediante *High-Frequency Trading* rispetto all'irrinunciabile principio di personalità della responsabilità penale.

2. Brevi cenni sul quadro normativo in materia di *market abuse*: l'abuso di informazioni privilegiate e la manipolazione del mercato.

Nell'ambito dell'ordinamento italiano, la disciplina fondamentale in materia di *market abuse* è contenuta nel d.lgs. 24 febbraio 1998, n. 58 (Testo Unico delle disposizioni in materia di intermediazione finanziaria, o T.U.F.) - come recentemente modificato dal d.lgs. 10 agosto 2018, n. 107[1] – il quale si prefigge obiettivi di tutela dell'utenza rispetto ad eventuali reati di abuso di mercato[2].

[1] Il d.lgs. n. 107/2018, relativo agli abusi di mercato, recepisce il Regolamento UE n. 596/2014, del 16 aprile 2014.
[2] La normativa di settore è stata originariamente introdotta nell'ordinamento italiano con la legge del 17 maggio 1991, n. 157, attuativa della

In particolare, il Titolo I-Bis, Parte V, dedicato agli Abusi di Mercato (artt. 180-187 *quaterdecies*), disciplina le interazioni tra i soggetti che operano sul mercato finanziario, regolando i principali aspetti dell'intermediazione finanziaria, con la finalità di assicurare l'integrità dei mercati finanziari e accrescere la fiducia degli investitori nei mercati stessi.

Sotto il profilo penale, i comportamenti che alterano e violano l'integrità dei mercati possono in via generale ricondursi a due gruppi: l'abuso di informazioni privilegiate (o *Insider Trading*)[3], disciplinato dall'art. 184 T.U.F. e la manipolazione del mercato che, qualora riguardi strumenti quotati o in corso di quotazione è disciplinata dall'art. 185 T.U.F., mentre negli altri casi è prevista dall'art. 501 c.p, rubricato "Rialzo e ribasso fraudolento di prezzi sul pubblico mercato o nelle borse di commercio"[4]; tale ultima ipotesi è a sua volta fattispecie comune rispetto al reato di aggiotaggio di cui all'art. 2637 c.c.

Il reato di abuso di informazioni privilegiate - il cui bene giuridico tutelato è rappresentato secondo parte della dottrina dalla parità conoscitiva degli informatori, ossia dalla parità di accesso alle informazione *price sensitive*[5] - consiste nell'immissione di ordini nel mercato ricorrendo ad informazioni privilegiate, in quanto tali non pubbliche e specifiche, idonee, se pubblicate, ad influenzare il prezzo di strumenti finanziari. Nel dettaglio, ai sensi dell'art. 184, comma primo, T.U.F. è prevista la punizione, con la reclusione da uno a sei anni e con la multa da euro ventimila a euro tre milioni, di chiunque, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio: a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime; b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato effettuato ai sensi dell'articolo 11 del regolamento UE n. 596/2014[6] (anche detto tipping); c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a)[7] (anche definito tuyautage).

L'art. 185 T.U.F., che punisce la "manipolazione del mercato" laddove le condotte riguardino strumenti quotati o in corso di quotazione, distingue invece tre condotte punibili, sanzionate con la pena della reclusione da uno a sei anni e la multa da euro ventimila a euro cinque milioni; la prima consiste nella diffusione di notizie false, vale a dire nella comunicazione di notizie che potrebbero alterare la realtà finanziaria in quanto non attendibili, inidonee o poco chiare[8] (cd. manipolazione del mercato di carattere informativo). La seconda condotta

Direttiva n. 89/592/CEE, con l'obiettivo di evitare che il possesso di informazioni privilegiate e il loro utilizzo potesse minacciare il regolare funzionamento del mercato e la sua integrità.

[3] Una definizione di informazione privilegiata è fornita dall'art. 7 del Regolamento UE n. 596/2014, secondo cui per informazione privilegiata si intende: "a) un'informazione avente un carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti o uno o più strumenti finanziari, e che, se resa pubblica, potrebbe avere un effetto significativo sui prezzi di tali strumenti finanziari o sui prezzi di strumenti finanziari derivati collegati; b) in relazione agli strumenti derivati su merci, un'informazione avente un carattere preciso, che non è stata comunicata al pubblico, concernente, direttamente o indirettamente, uno o più di tali strumenti derivati o concernente direttamente il contratto a pronti su merci collegato, e che, se comunicata al pubblico, potrebbe avere un effetto significativo sui prezzi di tali strumenti derivati o sui contratti a pronti su merci collegati e qualora si tratti di un'informazione che si possa ragionevolmente attendere sia comunicata o che debba essere obbligatoriamente comunicata conformemente alle disposizioni legislative o regolamentari dell'Unione o nazionali, alle regole di mercato, ai contratti, alle prassi o alle consuetudini, convenzionali sui pertinenti mercati degli strumenti derivati su merci o a pronti; c) in relazione alle quote di emissioni o ai prodotti oggetto d'asta correlati, un'informazione avente un carattere preciso, che non è stata comunicata al pubblico, concernente, direttamente o indirettamente, uno o più di tali strumenti e che, se comunicata al pubblico, potrebbe avere un effetto significativo sui prezzi di tali strumenti o sui prezzi di strumenti finanziari derivati collegati; d) nel caso di persone incaricate dell'esecuzione di ordini relativi a strumenti finanziari, s'intende anche l'informazione trasmessa da un cliente e connessa agli ordini pendenti in strumenti finanziari del cliente, avente un carattere preciso e concernente, direttamente o indirettamente, uno o più emittenti o uno o più strumenti finanziari e che, se comunicata al pubblico, potrebbe avere un effetto significativo sui prezzi di tali strumenti finanziari, sul prezzo dei contratti a pronti su merci collegati o sul prezzo di strumenti finanziari derivati collegati".

[4] Art. 501 c.p. "*Chiunque, al fine di turbare il mercato interno dei valori o delle merci, pubblica o altrimenti divulga notizie false, esagerate o tendenziose o adopera altri artifici atti a cagionare un aumento o una diminuzione del prezzo delle merci, ovvero dei valori ammessi nelle liste di borsa o negoziabili nel pubblico mercato, è punito con la reclusione fino a tre anni e con la multa da cinquecentosedici euro a venticinquemilaottocentoventidue euro*".

[5] Secondo altra parte della dottrina il bene giuridico tutelato sarebbe invece rinvenibile nel corretto funzionamento dell'integrità del mercato. Il tema è stato oggetto di ampio dibattito; si rinvia sul tema a Carriero (1992), pp. 2 ss.; Bartulli (1992), pp. 163 ss.; Arenaccio *et al.* (2016), p. 53; Padovani (1995), p. 641. Il riferimento al regolare funzionamento del mercato è inteso invece correttamente come scopo di disciplina; cfr. Seminara (2000), p. 514.

[6] Lettera così modificata dall'art. 4 del d.lgs. n. 107/2018.

[7] Il comma 3 *bis* dell'articolo è stato dapprima aggiunto dall'art. 1, comma 17, del d.lgs. n. 101 del 17 luglio 2009 e poi modificato dall'art. 4 del d.lgs. n. 107/2018. Il comma quarto è stato abrogato dall'art. 4 del d.lgs. n. 107 del 10 agosto 2018.

[8] La notizia in questione, come disposto dall'art. 181 T.U.F., deve essere "sufficientemente specifica".

riguarda le cd. operazioni simulate. La terza condotta, ricalcando il dettato di cui all'art. 2637 c.c., si riferisce al compimento di tutti gli "altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari" (in questi ultimi due casi si parla anche di manipolazione del mercato di carattere operativo o manipolativo).

Il reato di manipolazione del mercato, il cui bene giuridico tutelato è rappresentato dalla corretta formazione del prezzo degli strumenti finanziari e, più in generale, dal corretto ed efficiente andamento del mercato finanziario[9], può dunque essere "informativo", allorquando avvenga attraverso la diffusione di informazioni false o fuorvianti con il fine di generare un certo rialzo o ribasso del prezzo di uno strumento finanziario, o "operativo", laddove si basi su strategie simulate o altri artifici, fondati prevalentemente sull'immissione di ordini in grado di alterare il naturale processo di formazione dei prezzi[10].

Il capo III del Titolo I-*bis* del d.lgs. n. 58/1998, come modificato per effetto del regolamento UE n. 596/2014, prevede inoltre l'applicazione di sanzioni amministrative ai sensi dell'art. 187 *bis*, rubricato "abuso e comunicazione illecita di informazioni privilegiate" e dell'art. 187 *ter* che disciplina la "manipolazione del mercato".

Come anticipato, la disciplina del *market abuse* è contenuta altresì nell'art. 2637 c.c., che rappresenta la disciplina di riferimento per il reato di aggiotaggio[11]. Tale disposizione è stata introdotta con il d.lgs. 11 aprile 2002, n. 61, con il quale sono confluite nello stesso articolo i reati di cui agli artt. 2628 c.c., 181 T.U.F. e 138 d.lgs. 1 settembre 1993, n. 385 (Testo Unico Bancario). L'articolo è stato ulteriormente modificato per effetto della legge 18 aprile 2005, n. 62, che recepiva la direttiva 2003/6/CE, poi abrogata, in materia di repressione degli abusi di mercato[12]. Anche l'art. 2637 c.c. prevede sia l'aggiotaggio informativo che quello manipolativo: il primo si sostanzia nella diffusione di notizie false, il secondo nel porre in essere operazioni simulate o altri artifici "concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari"[13].

In considerazione della portata sovranazionale della materia, la disciplina è stata oggetto di attenzione anche da parte del legislatore europeo; è in questo contesto che si inserisce inizialmente la Direttiva 2003/6/CE nota come *Market Abuse Directive*, che provvedeva a riformare l'intera materia e che è stata recepita in Italia con la l. n. 62/2005 che, tra le altre cose, ha previsto l'assegnazione di poteri di controllo e sanzionatori anche ad autorità pubbliche di vigilanza, come la Consob, in grado di monitorare le informazioni rese dagli emittenti e l'andamento degli scambi sui mercati finanziari[14].

La Direttiva 2003/6/CE è stata tuttavia successivamente abrogata dalla direttiva 57/2014, del 16 aprile 2014 (anche conosciuta come Mad II), relativa alle sanzioni penali in materia di abusi di mercato[15].

Orbene, numerose sono le problematiche che tradizionalmente si sono poste con riferimento alla disciplina dell'abuso di mercato. In questa sede ci si limita a ricordare che la materia è frutto di una stratificazione normativa e si è da sempre contraddistinta per l'anticipazione della soglia di tutela, per una disciplina sanzionatoria severa, nonché per il ricorso alla tecnica

[9] Sul tema, di recente, Cass., Sez. V, 13 settembre 2016, n. 3836. In dottrina, sul tema, Antolisei (2000), pp. 525 ss.; Mucciarelli (2002), pp. 431 ss.; Musco (2007), pp. 282 ss.

[10] Le strategie di manipolazione operativa sono diverse ma, in via generale, possono suddividersi in due gruppi, a seconda che gli ordini e le operazioni siano idonei a fornire *imput* falsi sul valore reale dello strumento finanziario, in modo da indurre gli altri partecipanti al mercato a realizzare a loro volta operazioni in grado di produrre ulteriori variazioni dei prezzi, funzionali anch'esse a favorire gli interessi del manipolatore (*misleading transaction*), o siano soltanto idonei a fissare valori di prezzo anomali ed utili agli interessi del manipolatore (*price positioning*).

[11] La portata applicativa di tale disposizione ha tuttavia subito nel tempo un notevole ridimensionamento a seguito delle variazioni apportare dalla legislazione speciale.

[12] Ai fini della consumazione del reato di aggiotaggio non è richiesta la verificazione della effettiva sensibile alterazione del prezzo degli strumenti finanziari, ma è sufficiente l'idoneità della condotta a produrre tale effetto.

[13] La disciplina nazionale in materia di abusi di mercato è contenuta altresì, tra le altre, nelle seguenti fonti: Regolamento Consob n. 11971/1999 (Regolamento Emittenti), Regolamento Consob n. 16191/2007 (Regolamento Mercati), Comunicazione Consob n. 0061330/2016, Delibera Consob n. 16839/2009, Delibera Consob n. 18406/2012. Inoltre il d.lgs. n. 58/1998 è ancora oggi oggetto di continue modifiche normative: si ricordano al riguardo il d.lgs. 14 novembre 2016, n. 224, per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE n. 1286/2014, nonché la l. 9 luglio 2015, n. 114, attuativa della Direttiva n. 2014/57/UE.

[14] Si rinvia anche a Basile (2016), pp. 271-282; Mucciarelli (2018a), pp. 5 ss.

[15] Per una ricostruzione della disciplina, anche in una prospettiva transnazionale, si rinvia altresì a Mucciarelli (2016), pp. 193 ss.; Quirici (2006), pp. 111 ss.; Preziosi (2008).

degli elementi normativi, spesso vaghi ed elastici[16].

Tra le questioni che sono stata affrontate dalla dottrina e dalla giurisprudenza si menzionano altresì il pericolo di una violazione del principio del *ne bis in idem*, in relazione ad un'eventuale sovrapposizione tra sanzioni penali (artt. 184 e 185 T.U.F.) e sanzioni amministrative che descrivono la medesima condotta (artt. 187 *bis* e 187 *ter* T.U.F.)[17], il rispetto del principio di proporzionalità, la difficoltà di incriminazione dell'*Insider* cd. secondario[18], le diverse prese di posizione in ordine alla configurazione di tali reati come fattispecie di pericolo concreto o astratto, nonché come reati propri[19] o comuni[20].

3. L'evoluzione tecnologia in materia di *market abuse*: gli algoritmi ad alta velocità.

Alle questioni brevemente evidenziate, storicamente dibattute in materia di *market abuse*, se ne aggiungono nel contesto odierno delle altre, strettamente condizionate dall'evoluzione tecnologica che ha investito anche il settore finanziario. Ci si riferisce in particolare all'emersione e al ricorso sempre più frequente a nuovi strumenti e modalità di investimento nel mercato, attività di *trading* basate sull'uso di algoritmi e programmi informatici[21], in genere molto complessi e sofisticati, che raccolgono ed elaborano informazioni e dati di mercato in tempo reale e avviano automaticamente, su varie piattaforme di negoziazione, ordini di acquisto e vendita di strumenti finanziari[22].

Cosicché, nel contesto odierno, buona parte delle operazioni di negoziazione finanziaria non appaiono più riconducibili a soggetti-persone fisiche (*slow traders*) e appare sempre più difficile distinguere l'azione umana da quella di elaboratori e programmi informatici che operano anche in condizioni di "autonomia" rispetto ad eventuali istruzioni impartite dagli investitori.

Orbene, quando i predetti *trading* algoritmici operano a velocità molto elevate prendono il nome di algoritmi di "nuova generazione", anche definiti *trading* ad alta frequenza o *high-frequency trading* (HFT)[23], le cui specificità rendono vieppiù complesse le sfide poste dall'emersione dei *trading* algoritmici di "prima generazione" nel mercato finanziario, sia in ragione della difficoltà di definirli, dovuta all'estrema eterogeneità che li caratterizza, sia in considerazione delle peculiari modalità di negoziazione attraverso cui operano[24]. Invero, con il ricorso agli HFT non solo la fase di *esecuzione* delle transazioni risulta interessata dall'evoluzione tecnologica ma anche, e soprattutto, la stessa *decisione* di compierle, che non risiede più nella determinazione di soggetti-persone fisiche, ma in calcoli matematici elaborati dagli stessi sistemi algoritmici in grado di assumere decisioni autonome[25].

---

[16] Sul tema si rinvia, per tutti, a Giavazzi (2009), pp. 801 ss.; Manno (2012), pp. 1 ss.; Mucciarelli (2000), pp. 932 ss.; Sgubbi (2008), pp. 3 ss.

[17] Sul punto, per tutti, Mucciarelli (2005), pp. 1472 ss.

[18] L'*insider trading* secondario si riferisce all'abuso di informazioni privilegiate compiuto da chi, a differenza dell'insider "primario", non vanta un accesso "istituzionale" all'informazione, ma ne viene a conoscenza in via indiretta.

[19] L'art. 185 T.U.F. esordisce con "Chiunque"; se *prima facie* sembrerebbe trattarsi di un reato comune, in effetti è difficile immaginare che la disposizione si rivolga alla generalità dei consociati, come soggetti in grado di "provocare una sensibile alterazione dei prezzi degli strumenti finanziari".

[20] Nel caso dell'aggiotaggio informativo, inoltre, si ricorda altresì la difficoltà di individuare con esattezza il *locus commissi delicti* e il *tempus commissi delicti*.

[21] Una definizione normativa di negoziazione algoritmica si rinviene nella Direttiva 2014/65/UE (cd. MiFID II), all'art. 4 §1, n. 39, secondo cui per *negoziazione algoritmica* deve intendersi lo scambio di "strumenti finanziari in cui un algoritmo informatizzato determina automaticamente i parametri individuali degli ordini, come ad esempio se avviare l'ordine, i tempi, il prezzo o la quantità dell'ordine o come gestire l'ordine dopo la sua presentazione, con intervento umano minimo o nullo".

[22] Sul tema Caivano *et al.* (2012), p. 7.

[23] L'art. 4, § n. 40 della Direttiva 2014/65/UE fornisce una definizione di "tecnica di negoziazione algoritmica ad alta frequenza" come "qualsiasi tecnica di negoziazione algoritmica caratterizzata da a) infrastrutture volte a ridurre al minimo le latenze di rete e di altro genere, compresa almeno una delle strutture per l'inserimento algoritmico dell'ordine: co-ubicazione, hosting di prossimità o accesso elettronico diretto a velocità elevata; b) determinazione da parte del sistema dell'inizializzazione, generazione, trasmissione o esecuzione dell'ordine senza intervento umano per il singolo ordine o negoziazione, e c) elevato traffico infragiornaliero di messaggi consistenti in ordini, quotazioni o cancellazioni".
La medesima direttiva disciplina altresì la negoziazione algoritmica ai sensi dell'art. 17.

[24] I *trading* ad alta frequenza possono configurarsi altresì come insieme di regole operative informatizzate in grado di fornire autonomamente indicazioni di acquisto e vendita.

[25] In questi termini Consulich (2018), p. 196.

Gli HFT compaiono nella scena del mercato finanziario mondiale intorno al 2000 e, come anticipato, si contraddistinguono per le velocità estremamente elevate con cui vengono compiute le operazioni negoziali di immissione, modifica e cancellazione di ordini. Si tratta di una modalità operativa che si è diffusa di recente, grazie al progresso tecnologico e che, in considerazione dei numerosi vantaggi arrecati, in termini di competitività, sta subendo nel panorama internazionale uno sviluppo rapido ed esponenziale. Invero, secondo uno studio condotto nel 2014 dalla *European Securities Market Authority* (ESMA), la quota di operazioni basate su tali tecniche nell'ambito della negoziazione sulle borse valori oscillava tra il 24% e il 43% del peso degli scambi finanziari operati[26].

L'HFT può essere in via generale definito come un programma informatico in grado di operare multiple transazioni finanziarie in un arco di tempo estremamente ridotto, caratterizzandosi dunque per la velocità di acquisizione, elaborazione e reazione rispetto ad un numero molto elevato di dati ed informazioni di mercato.

Tale capacità operativa è resa possibile sia grazie allo sviluppo di *software, hardware* e specifiche tecnologie particolarmente innovative, sia all'utilizzo di servizi che riducono il periodo di cd. latenza, ossia il lasso temporale che intercorre tra la *decisione* di compiere un'operazione finanziaria e la sua *esecuzione* sul mercato; importanza centrale assume per esempio, da questo punto di vista, la peculiare collocazione fisica assunta dagli *hardwares* che supportano gli HTF, i quali sono posti in prossimità del *server* dei mercati finanziari presso i quali tali programmi algoritmici sono destinati ad operare, cosicché lo spazio che l'impulso elettrico deve percorrere per giungere presso la piattaforma elettronica risulta maggiormente ridotto (tale caratteristica è conosciuta come cd. *co-location*)[27].

Considerato il basso "periodo di latenza" e la rapidità con cui operano, gli HTF sono quindi in grado, in pochi millisecondi, di compiere una transazione e liquidarla, nonché di modificare o cancellare più volte un ordine, di acquisto o vendita, subito dopo averlo immesso nel mercato, al fine di adeguarlo immediatamente ai cambiamenti intervenuti nel frattempo sul mercato 28.

Dunque, come ben espresso da una parte della dottrina, gli operatori algoritmici dispongono di un enorme "vantaggio competitivo, di carattere conoscitivo", dovuto alla loro superiorità in termini di "velocità operative"; in questo modo, dalla concorrenza *nei* mercati si passa alla concorrenza *tra* mercati istituzionali e mercati di nuova generazione[29].

Gli HTF effettuano inoltre continuamente delle opzioni tra più alternative possibili e generano sempre nuove occasioni di scelta attraverso la capacità di elaborazione critica di una quantità di informazioni certamente al di fuori della portata di un investitore-persona fisica. In questo modo, gli stessi sono perfino in grado di prevedere in anticipo l'andamento del mercato a breve termine, così da trarne ogni possibile beneficio economico.

Senonché, una delle caratteristiche che in questa sede maggiormente interessano è rappresentata dal fatto che, diversamente dagli algoritmi di prima generazione, i *trading* ad alta frequenza risultano altresì capaci di apprendere dal contesto in cui operano, modificando di conseguenza le proprie strategie operative. Gli HFT sono dunque progettati per reagire alle variazioni del contesto in cui agiscono, senza la necessità di ricevere istruzioni aggiuntive rispetto a quelle inizialmente impartite dal programmatore-persona fisica[30].

Oltre a rappresentare scelte "autonome", le decisioni di investimento degli HFT reagisco-

[26] *European Security and market abuse* (ESMA), *Economic Report. High-frequency trading activity in EU equity markets*, n. 1/2014, p. 4. In base a studi condotti nel 2011 il ricorso agli HTF variava tra il 40% e il 70% negli USA, attestandosi intorno al 10%, in crescita, nei paesi asiatici; v. Gomber *et al.* (2011). Per una ricostruzione storica delle ragioni che hanno condotto ad una rapida diffusione degli HTF si rinvia anche a Alvaro e Ventoruzzo (2016), pp. 417 ss.

[27] Al riguardo, nonostante i soggetti che operano con gli HFT (*high-frequency traders* - HFTr) costituiscano una categoria eterogenea, per cui risulta difficile fornirne una definizione unitaria e predisporre una disciplina adeguata, è tuttavia possibile individuare talune caratteristiche comuni. In primo luogo gli HFTr, grazie all'utilizzo di supporti informatici *hardware* e *software* sofisticati, sono in grado di inviare alle piattaforme di negoziazione molti ordini in un solo secondo. Inoltre, gli HFTr operano solitamente con titoli caratterizzati da una maggiore liquidità, per cui appare agevole disinvestire più rapidamente. Infine, poiché la velocità di negoziazione rappresenta un fattore centrale, gli HFTr ricorrono a tecnologie innovative che consentono di raggiungere velocità prossime a quella della luce; gli HTF sono infatti in grado di coprire in un millisecondo la distanza di circa 300 km. Una ricostruzione del tema è reperibile anche sul sito della Consob: *http://www.consob.it/web/investor-education/mercati-finanziari*. Sul tema anche Puorro (2013), pp. 10 ss.

[28] Gli *High-Frequency Traders* (HFTr), in un secondo, possono inviare alle piattaforme di negoziazione fino a 5.000 ordini. La cancellazione degli ordini avviene in modo frequente: per questo motivo l'operatività degli HFTr è spesso caratterizzata da un elevato rapporto tra ordini inviati e transazioni effettivamente realizzate (*order-to-trade ratio*).

[29] In questi termini, Consulich (2018), cit., p. 199.

[30] Si rinvia anche a Alvaro e Ventoruzzo (2016), cit., pp. 417 ss.

no a *imput* del mercato che prescindono dalle variabili economiche comunemente condivise e ritenute solitamente rilevanti per gli investitori fisici; ci si riferisce per esempio al valore effettivo dei titoli finanziari, alla situazione dell'emittente o alle condizioni del mercato di riferimento.

Gli operatori algoritmici analizzano e sfruttano, invece, le oscillazioni e gli scostamenti, spesso minimi, dei titoli, approfittando dei disallineamenti temporali nell'esecuzione delle transazioni compiute dagli altri intermediari fisici o degli infinitesimi ritardi operativi nella gestione dei mercati, o ancora, reagendo in base al numero delle volte in cui il nome dello strumento finanziario compare nei circuiti di diffusione di informazioni e sulle piattaforme di comunicazione di cui usufruiscono gli operatori[31].

Orbene, considerate le peculiarità che connotano gli HFT, la loro rapida diffusione nel mercato ha sollevato un'attenzione crescente, soprattutto da parte delle autorità di vigilanza che si sono interrogate in merito ad eventuali rischi e conseguenze che l'uso di HFT possa determinare all'interno del mercato.

Invero, a titolo di esempio, il ricorso a tali strumenti potrebbe destabilizzare i mercati, innescando *shock* endogeni: si pensi, ad esempio, ad un danno operativo (come un malfunzionamento) che, influenzando a sua volta le scelte e le strategie degli altri *high-frequency traders* (HFTr), crei un immediato effetto a catena, con rilevanti ripercussioni sull'intero mercato.

La capacità offensiva degli operatori algoritmici e le dinamiche distorsive cui possono dar luogo sono peraltro in grado di manifestarsi anche in assenza di danni operativi.

Si pensi al *flash crash*, fenomeno di improvviso e rapido ribasso dei prezzi, con conseguente 'rimbalzo' degli stessi nel giro di un arco temporale di pochi istanti, senza che l'oscillazione sia in alcun modo ragionevolmente riconducibile ad un mutamento del valore fondamentale del titolo o alla condizione contingente del mercato[32]. Ecco emergere una connessione tra *flash crashes* e operatori algoritmici[33]; questi ultimi infatti agevolano e rendono possibili vorticose oscillazioni dei prezzi di titoli quotati, cui conseguono peraltro ingenti benefici a favore di taluni soggetti che si avvantaggiano di tale turbativa[34].

Orbene, considerata l'eterogeneità delle forme in cui possono manifestarsi le operazioni sul mercato ricorrendo agli HTF, appare difficile definire il fenomeno in modo esaustivo e univoco. Tuttavia, è possibile distinguere tre strategie generali: quella di *market making*[35], l'ar-

[31] Mcgowan (2010), pp. 1 ss.

[32] Si pensi al *flash crash* del 6 maggio 2010, in cui mercati azionari USA hanno perso oltre il 10% in pochi minuti per poi recuperare rapidamente nella stessa giornata. In quella circostanza l'operare degli HFT ha amplificato il ribasso dei prezzi, come analizzato anche in base ad alcuni studi della SEC (*Securities and Exchange Commission*); sul tema Caivano *et al.* (2012), p. 17; Barrales (2012), pp. 1199 ss.; Puorro (2013), cit., pp. 26 ss.; Strampelli (2014), pp. 991 ss.

[33] Si pensi al riguardo a quanto avvenne nel corso di quindici minuti sui mercati finanziari americani in occasione del *flash crash* del 23 aprile del 2013; a seguito della falsa notizia di un attentato a Barack Obama, gli HFT hanno processato la notizia prima di ogni altro operatore, intuendo un effetto ribassista sui mercati e, dunque, anticipandone la verificazione e amplificandone la portata. Nell'arco di quindici minuti gli operatori algoritmici maturarono 600 milioni di dollari di profitti.

[34] Tra i rischi e gli effetti che il ricorso agli HFT può determinare sulla stabilità dei mercati si menziona anche la capacità di incidere sulla volatilità dei titoli e sull'aumento della liquidità dei titoli negoziati (*ghost liquidity*). Con riferimento al mercato italiano, un recente studio condotto dalla Consob mostra come, tra il 2011 e il 2013, un incremento del livello di attività HFT abbia determinato un notevole incremento della volatilità dei rendimenti giornalieri; un incremento del 10% del peso degli HFT "puri" (ossia degli operatori che svolgono HFT come attività principale) sul totale degli scambi ha portato a un aumento della volatilità (nell'arco di un giorno) tra il 4% e il 6%. Per una descrizione del fenomeno v. anche Consob, Mercati finanziari, consultabile all'indirizzo *http://www.consob.it/web/investor-education/mercati-finanziari*.
La diffusione degli HFT può altresì ripercuotersi sul processo di formazione dei prezzi; infatti, gli HFTr adottano strategie di breve periodo per cui gli ordini da loro emessi si basano sull'osservazione di ciò che accade sul mercato in un determinano istante. Scarsa considerazione viene data, invece, alle variabili economiche tipicamente prese in considerazione, che guidano solitamente scelte di investimento di lungo periodo. Ciò potrebbe determinare un allontanamento dei prezzi di mercato dai "fondamentali economici", riducendo la capacità del prezzo di un titolo di dare atto della condizione della società che lo ha emesso.
Infine, la partecipazione degli HFTr ai mercati finanziari può rappresentare un problema in termini di equo accesso al mercato. Non tutti i partecipanti al mercato possono infatti ricorrere alle tecnologie HFT, che richiedono notevoli investimenti in termini di infrastrutture tecnologiche, informatiche e di capitale umano.
Gli operatori che vi facciano ricorso godono pertanto di un vantaggio oggettivo (anche in termini di velocità) rispetto agli altri. Quest'ultimo aspetto è peraltro disciplinato dalla Direttiva 2014/65/UE.
Anche alla luce delle considerazioni espresse, i principali studi che hanno analizzato l'impatto dell'HFT sui mercati sono giunti a risultati contrastanti: in alcuni casi hanno portato a concludere che l'operatività degli HFT possa produrre effetti benefici per il mercato. In altri casi, hanno mostrato che le caratteristiche operative degli HFT potrebbero danneggiare il mercato, specialmente in momenti di turbolenza.

[35] Attraverso il *market making* si fornisce liquidità agli strumenti negoziati sulle diverse piattaforme, garantendo la disponibilità a negoziare tali strumenti e proponendo prezzi in acquisto e vendita; in questo contesto gli HTF determinano la formazione di profitti attraverso l'inserimento e la cancellazione continua di ordini.

bitraggio statistico[36] e la cd. *liquidity detection*[37].

4. Il nuovo volto del *market abuse*: le interazioni tra il sistema degli algoritmi ad alta velocità e la disciplina vigente.

Alla luce di quanto detto, si pongono a questo punto talune questioni che, in considerazione del peculiare modo di atteggiarsi e di operare degli HFT, assumono importante rilievo in ambito penalistico.

Senza addentrarci nel tema del riconoscimento, più o meno auspicabile, di una soggettività giuridica di diritto penale attribuibile ad entità artificiali[38], ambito che pur pone delicati problemi, si ritiene di affrontare talune questioni in qualche modo ad essa riconducibili. In proposito, considerata l'evoluzione tecnologica che ha interessato il mercato finanziario, ci si chiede in primo luogo se i delitti tradizionalmente previsti in materia di abuso di mercato, riconducibili per lo più a scelte e comportamenti di investitori-persone fisiche (*slow traders*), possano oggi ritenersi applicabili anche alle nuove configurazioni in cui le fattispecie di reato possono concretamente manifestarsi.

In particolare, specialmente con riferimento al reato di abuso di informazioni privilegiate, di cui all'art. 184 T.U.F., l'avvento degli HFT finisce con il porre in discussione la stessa validità di alcune nozioni fondamentali del diritto penale finanziario; più precisamente, occorre prendere atto della potenziale trasformazione di alcuni concetti portanti, come quello di "investitore ragionevole" di cui all'art. 181 T.U.F., ora art. 180, *lett. b-ter)*, T.U.F.[39], tenendo altresì in considerazione l'impatto di tali nuovi concetti sull'applicazione delle fattispecie incriminatrici che tipicamente vengono in rilievo in questo settore[40]. Nella medesima prospettiva, il nuovo volto assunto dal mercato finanziario a contatto con l'evoluzione tecnologica potrebbe indurre a chiedersi altresì cosa si intenda oggi per "informazione privilegiata". Tali questioni si pongono, in particolare, con riferimento al reato di abuso di informazioni privilegiate, in quanto le scelte operate dagli HFT possono apparire, oltre che "autonome", anche ingiustificate, quanto meno nell'ottica del "soggetto modello" indicato all'art. 180, *lett. b-ter)*, T.U.F., ossia l' "investitore ragionevole"; invero, come anticipato, gli HFT reagiscono a *imput* del mercato privi, apparentemente, di rilevanza economica, prescindendo dal valore dei titoli finanziari e dalle condizioni di mercato tradizionalmente prese in considerazione dagli investitori-persone fisiche e sfruttano invece le oscillazioni minime dei titoli, approfittando dei disallineamenti temporali nell'esecuzione delle transazioni compiute dagli altri operatori finanziari o dei ritardi operativi connaturati ai mercati[41]. A tali considerazioni conseguono pertanto delle implicazioni sul piano del significato stesso da attribuire al concetto di "informazione previlegiata" e di "informazione finanziaria" in generale[42].

Da questa prospettiva, "ad essere coinvolte potrebbero essere quindi le stesse architravi della tutela penale contro gli abusi di mercato"[43]; la presenza di HTF e la loro maggiore "competenza" potrebbe infatti determinare, tra le altre cose, un ampliamento "incontrollabile"

[36] Con tale strategia di *trading*, che ricorre all'analisi statistica delle fluttuazioni del prezzo degli strumenti finanziari, riconducibile al "*trading* di coppia", (*pair trading*), vengono assunte posizioni di segno opposto su strumenti finanziari tra loro correlati.

[37] Strategia che si fonda sull'osservazione degli altri partecipanti al mercato, in modo da desumerne in anticipo le strategie e agire di conseguenza.

[38] Sul tema si richiama la Risoluzione del Parlamento Europeo del 16 febbraio 2017.

[39] La definizione di "investitore ragionevole" era prima contenuta nell'art. 181, comma quarto, T.U.F., poi soppresso dall'art. 4 del d.lgs. 10 agosto 2018, n. 107 e dunque trasposto nella *lett. b-ter)* dell'art. 180, comma primo, T.U.F., che rinvia all'art. 7 del Regolamento UE n. 596/2014.
In materia, anche Consulich e Mucciarelli (2016), pp. 179 ss.

[40] Si rinvia a Consulich (2018), cit., p. 198, secondo cui occorrerebbe altresì interrogarsi sui "protocolli di reazione punitiva" più adeguati rispetto alle turbative del mercato riconducibili agli HFT.
Oggetto di riflessione è in questo contesto lo stesso modello di imputazione della responsabilità, che passa attraverso la definizione del soggetto cui attribuire penalmente il fatto di reato, la cui concreta manifestazione dipende anche da scelte autonome dell'algoritmo, quale operatore economico dotato di capacità di apprendimento e decisione.

[41] In altri termini si tratta di scelte di investimento che non reagiscono al cd. *"valore fondamentale"* degli strumenti finanziari. Così gli HFT, che svolgono un ruolo centrale nell'ambito degli scambi di titoli quotati, sono influenzati limitatamente o in misura nulla dai dati disponibili che riguardano gli strumenti finanziari oggetto di investimento, i loro emittenti e il mercato.

[42] Si tratta di un'implicazione che agisce sia sulla sussunzione di tali operatori entro la disposizione normativa, sia sulla definizione degli elementi normativi essenziali ai fini dell'integrazione della figura di reato in questione.

[43] Consulich (2018), cit., p. 212.

della nozione di informazione privilegiata, con la conseguente proliferazione delle occasioni di "abuso" della stessa[44], sia in ragione del diverso significato da attribuire alla stessa "informazione", sia a causa della difficoltà di adeguare i controlli ad un flusso di informazioni tanto elevato.

In altri termini, in considerazione del fatto che gli HFT prescindono dall'analisi di informazioni considerate rilevanti per gli investitori-persone fisiche e reagiscono invece a variabili che non sono apparentemente dotate di rilevanza economica, potrebbe darsi luogo ad una enorme estensione dei doveri di comunicazione e astensione degli operatori e, conseguentemente, ad una paralisi delle attività di controllo e vigilanza; inoltre, dal momento che gli HFT elaborano informazioni e dati che appaiono trascurabili per ogni altro operatore economico che non sia un HFT, le transazioni compiute non sono "informative" in quanto non veicolano nessuna informazione in ordine al valore intrinseco dei titoli oggetto di scambio o all'andamento del mercato. In questo modo, si ribaltano alcuni principi su cui si fonda il diritto penale finanziario, legati anche al fatto che i comportamenti degli investitori cessano di rappresentare, a loro volta, informazioni per gli altri soggetti del mercato[45]"; inoltre, è tale *modus agendi* degli HFT che spesso può indurre gli operatori finanziari a prediligere piattaforme di negoziazione "meno trasparenti" (cd. *Dark pools*) e ad allontanarsi dal mercato istituzionale, evitando in questo modo che i propri "comportamenti" possano essere studiati e strumentalizzati a fini di vantaggio degli HFT.

5. L'*High-Frequency Trading* e il rispetto del principio di personalità della responsabilità penale.

Un secondo ordine di questioni riguarda più propriamente il reato di manipolazione del mercato sia in relazione alle tensioni che possono intervenire rispetto al principio di personalità della responsabilità penale, sia in ragione della diretta incidenza degli HFT sulle quotazioni dei titoli, anche di carattere distorsivo. Al riguardo, la teoria economica ha infatti individuato alcune "strategie" che si sono mostrate in grado di generare una rappresentazione distorta delle negoziazioni, così aprendo la via a potenziali manipolazioni di mercato: si pensi al cd. *smoking*[46], allo *spoofing*[47], al *layering*[48], al *front running*[49], alle *quote stuffing*[50], al *pinging*[51], alle tecniche di "*order flow detection*"[52], nonché alle evoluzioni del *Pump and dump* (come la pratica del cd. *momentum ignition*)[53]. Inoltre, occorre tenere in considerazione la stretta connessione che intercorre tra manipolazione del mercato ed informazione finanziaria e le conseguenze che ne derivano[54].

Orbene, nei reati di *market abuse* realizzati tramite HFT occorre preliminarmente definire il soggetto cui attribuire un'eventuale responsabilità penale per un fatto che, *prima facie*, sem-

[44] In questi termini Consulich (2018), cit., p. 214 s; Strampelli (2014), cit., pp. 1038 ss.;
[45] Hu (2012), pp. 1705 ss.
[46] Prevede di "richiamare" altri operatori con offerte, subito modificate a prezzi più svantaggiosi.
[47] Prevede l'immissione e la cancellazione di ordini per indurre gli operatori a ritenere che sia iniziata una certa fase di tendenza. In particolare, se l'intenzione dell'HFT è comprare un titolo sul mercato, per ottenere migliori condizioni di acquisto, immetterà una serie di ordini di vendita, con offerte per lo più superiori al miglior prezzo di vendita presente sul mercato, al fine di indurre gli altri investitori a credere che sia cominciata una fase di ribasso del titolo. L'elevata velocità dell'HFT gli consente di cancellare poi tali ordini prima che siano eseguiti e, nel frattempo, di immettere un ordine di acquisto a prezzi influenzati dalla pressione determinata dalla precedente offerta, a svantaggio degli altri investitori.
[48] Si tratta dell'inserimento simultaneo di un ordine di acquisto nascosto e di un ordine di vendita visibile.
[49] In questo modo si sfrutta la posizione di asimmetria informativa in cui versa il "mandante". Il *broker* sfrutta la conoscenza dell'ordinativo effettuato, che se di importo elevato modificherà il prezzo dello strumento interessato e immediatamente prima di immettere l'ordine sul mercato acquista, a titolo personale, il titolo in questione (se l'ordinativo è di acquisto) o lo vende (in caso contrario). In tal modo, trarrà profitto dall'aumento del prezzo del titolo (nel caso di acquisto) o eviterà di subire perdite per la diminuzione dello stesso (nel caso di vendita).
[50] Immissione e contestuale cancellazione di migliaia di ordini in quantità tali da determinare un rallentamento nel funzionamento dei sistemi di *trading* degli altri operatori.
[51] Inserimento di piccole proposte di acquisto per scoprire i comportamenti degli altri *trader*.
[52] Identificazione e sfruttamento di blocchi di ordini.
[53] Tipologia di frode che consiste nel far aumentare artificialmente il prezzo di un'azione a bassa capitalizzazione al fine di vendere titoli azionari acquistati a buon mercato ad un prezzo superiore.
[54] Nell'ambito del reato di manipolazione di mercato si determinare un'alterazione del patrimonio di informazioni di cui gli altri investitori dispongono, compromettendo la loro capacità di assumere decisioni "consapevoli". In questo contesto anche lo stesso comportamento illecito, nel momento in cui si manifesti nel mercato, esprime una componente comunicazionale e "informativa", oltre all'informazione che veicola; tuttavia agendo gli HFT in funzione di variabili considerate "trascurabili" per il resto del mercato, l'informazione dagli stessi fornita attraverso le negoziazioni operate non è una informazione.

bra dipendere principalmente da scelte "autonome" dell'algoritmo stesso, in quanto soggetto economico dotato di capacità decisionale e di apprendimento. Occorre, quindi, ricostruire i profili di responsabilità e i possibili meccanismi di imputazione dell'illecito alla persona fisica che ricorra a tali modalità operative, sia essa il produttore, l'intermediario finanziario, l'utilizzatore o il beneficiario finale.

In effetti, se il comportamento dell'algoritmo sul mercato è certamente in radice influenzato dalle istruzioni inizialmente impartite dall'utilizzatore, è dall'interazione tra l'algoritmo e l'ambiente economico mutevole in cui lo stesso si colloca che può scaturire una decisione di investimento assolutamente "imprevedibile" nel momento in cui il programma algoritmico è stato generato e immesso sul mercato. In altre parole, in termini penalistici, ci si potrebbe trovare di fronte ad una rottura del rapporto di "*autoria*" tra operazione finanziaria e soggetto agente, potendosi riferire la prima al secondo solo in via "tendenziale"[55].

Invero, come anticipato, gli HTF si distinguono per il fatto di essere *decision makers*, manifestando una vera e propria "autonomia operativa" rispetto ai soggetti nel cui interesse operano[56].

In particolare, nell'ambito del contesto delineato e con specifico riferimento al delitto di manipolazione del mercato, si possono distinguere due ipotesi problematiche, a seconda che il comportamento tenuto dal programmatore iniziale sia lecito o illecito.

Nella prima ipotesi, laddove il programmatore o l'utilizzatore iniziale agiscano lecitamente, l'HFT può finire per reagire in modo distorsivo rispetto ad una situazione occasionale e contingente, come per esempio un'instabilità delle quotazioni. L'evento offensivo si collocherebbe, in questo caso, ad una distanza tale dalla condotta iniziale del programmatore o dell'intermediario finanziario che utilizzi l'algoritmo, da risultare difficile ricondurre la perturbazione delle negoziazioni ad una responsabilità dell'operatore iniziale; non è agevole pertanto imputare la responsabilità penale al soggetto-persona fisica che abbia agito, a monte, nella programmazione del *trading*, se non verificando la possibilità di ricorrere al meccanismo imputativo di cui all'art. 40, comma secondo, c.p..

Inoltre, in considerazione del fatto che l'integrazione del reato di manipolazione del mercato richiede la diffusione di notizie false o che siano poste in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, mancherebbe in questo caso la tipicità del predetto reato: la persona fisica, infatti, inserisce nel mercato degli algoritmi che solo in un momento successivo, interagendo con una determinata situazione contingente del mercato, generano e amplificano una distorsione dei prezzi determinata da altre cause.

Occorre poi riflettere sull'opportunità di ricostruire il concetto di "artifici", *ex* art. 185 T.U.F., laddove "posti in essere dagli algoritmi", anche attraverso una più precisa elencazione delle situazioni-tipo o mediante esempi, come avviene ai sensi dell'art. 12 del Regolamento UE n. 596/2014.

Di più difficile soluzione risulta la seconda ipotesi che può venire in considerazione, laddove il programmatore iniziale agisca illecitamente.

In tale ipotesi, infatti, l'HFT opera mettendo in pratica le istruzioni illecite impartite dal programmatore o dall'intermediario finanziario "a monte", ossia nel momento in cui l'algoritmo venga immesso nel mercato.

Orbene, se *prima facie* sembrerebbe in questo caso più agevole ricondurre il reato di manipolazione del mercato al programmatore, in effetti l'attribuzione di una responsabilità a tale soggetto non è così automatica. Invero, le eventuali informazioni impartite dal programmatore hanno natura generale, indicando all'algoritmo il modello di comportamento finanziario da seguire, ma non anche la tipologia e l'identità del titolo da colpire, il momento in cui farlo e secondo quali modalità e combinazioni con il contesto[57].

È dunque possibile che il soggetto-persona fisica non abbia una piena rappresentazione e volizione delle operazioni compiute in concreto dall'algoritmo.

In altri termini, potrebbe difettare in questo caso "il dolo del fatto" della persona fisica, venendo meno la rappresentazione e volontà delle concrete modalità attraverso cui si manifesta

[55] In questi termini Consulich (2018), p. 207; Yadav (2014), p. 37.
[56] Scopino (2015), p. 458.
[57] Consulich (2018), cit., p. 219, che sull'irrilevanza del cd. *dolus generalis*, come volizione in termini astratti e generici dell'evento naturalistico a prescindere dagli altri elementi del fatto come storicamente verificatosi, rinvia a sua volta a Grosso *et al.* (2017), p. 332. In giurisprudenza Cass., 18 marzo 2003, n. 16976, più di recente, Cass., 17 novembre 2015, n. 15774.

il reato.

Tale questione finisce per spostare l'oggetto del discorso sull'esatta individuazione dell'oggetto del dolo, tema storicamente interessato da un ampio dibattito dottrinale.

Invero il dolo è, come è noto, il termine linguistico che ha storicamente espresso il più intenso legame psicologico tra il fatto ed il suo autore.

Oggetto del dolo è il fatto tipico ossia l'insieme degli elementi obiettivi positivamente richiesti per l'integrazione delle singole figure di reato e la mancanza degli elementi negativamente richiesti per l'integrazione delle singole figure di reato. Il dolo deve quindi abbracciare tutte le *component* in cui il fatto tipico può articolarsi: condotta, circostanze antecedenti o concomitanti all'azione tipizzata, evento, elementi normativi del fatto.

L'oggetto del dolo non è quindi identificabile esclusivamente nell'evento in senso naturalistico ma coinvolge tutti gli elementi del fatto storico che costituisce il reato. Da ciò può derivare la difficoltà di ricostruire un legame effettivo, sul piano psicologico, tra la condotta del programmatore e l'evento[58].

Pertanto, alla luce di quanto detto, dopo aver individuato il soggetto cui attribuire la responsabilità penale, si tratterebbe di verificare se e a che titolo tale soggetto sia chiamato a rispondere[59], se a titolo di dolo omissivo, riconoscendo eventualmente una posizione di garanzia *ex* art. 40, comma secondo, c.p. in capo al programmatore iniziale o all'investitore per non aver posto in essere un comportamento doveroso, o per carenze di controlli[60]. In ogni caso, sono indubitabili le numerose difficoltà cui si andrebbe incontro in sede di accertamento del reato, potendo incorrersi in ipotesi di *probatio diabolica*.

La questione è dunque quella di individuare il titolo soggettivo di imputazione a carico della persona fisica[61].

Orbene, in questi casi, al fine di ipotizzare talune soluzioni rispetto alle problematiche evidenziate, si ritiene di condividere il pensiero di quella parte della dottrina che si è riferita principalmente a due diversi meccanismi imputativi: il ricorso al sistema dell'*actio libera in causa* e l'implementazione della disciplina della responsabilità dell'ente, attraverso una valorizzazione dell'art. 8 del d.lgs. 8 giugno 2001, n. 231[62].

[58] Sul tema si ricordano le parole di Falcinelli (2018), p. 5, secondo cui "Le alterne stagioni dell'impostazione esegetica assunta come conferente per l'identificazione di "questo" dolo – probabilità piuttosto che possibilità del risultato; accettazione e approvazione dell'evento piuttosto che speranza della non produzione – convincono *a fortiori* che nella formula "volontà dolosa/decisione per il fatto" sia da leggere una clausola di rinvio materiale-recettizio ad una cultura giuridica fondata sul sapere del sistema, prodotto delle scienze di volta in volta contemporanee".

[59] Con riferimento specifico all'imputazione del reato di cui all'art 501 c.p., inoltre, il soggetto non potrebbe essere chiamato a rispondere neanche a titolo di dolo eventuale, in considerazione del fatto che la fattispecie si presenta a dolo specifico.

[60] Sul tema Magro (2014), p. 514.
Con riferimento alla possibilità di attribuire una responsabilità agli operatori finanziari *ex* art. 40, comma secondo, c.p., si rinvia anche all'art. 114 T.U.F. e all'art. 22 *ter* della Direttiva 2014/65/UE che prevedono in capo a tali soggetti una serie di obblighi di comunicazione, nonché all'art. 16 del Regolamento EU n. 596/2014 in materia di prevenzione e individuazione degli abusi di mercato.
Per quanto attiene alla possibilità di imputare tali reati al soggetto-persona fisica a titolo di colpa, occorre inoltre ricordare che i reati di *market abuse* di cui agli artt. 184 e 185 T.U.F. non prevedono le corrispondenti fattispecie colpose. Al riguardo si segnala tuttavia che la Direttiva 2014/57/UE introduce, ai sensi del considerando n. 21, la possibilità per gli Stati membri di stabilire che la manipolazione del mercato commessa con grave colpa o negligenza costituisca reato.
E' inoltre previsto un obbligo di controllo anche per gli investitori in materia di informazioni privilegiate ai sensi del considerando 36 del Regolamento UE n. 596/2014.

[61] Analoghe problematiche si sono poste anche con riferimento alle intelligenze artificiali (AI). In questo caso più semplice è la soluzione per l'ipotesi dolosa, in quanto l'azione "volontaria" dell'operatore informatico rinvia ad una responsabilità dell'uomo, in quanto "l'azione del robot si indentifica e rappresenta una *longa manus* della persona umana". Così non emergono criticità in ordine al riconoscimento di una responsabilità penale dell'operatore se quest'ultimo intenzionalmente e consapevolmente programmi AI in modo che questo commetta reati. Più complessi i casi in cui l'uso di un AI provochi un danno indesiderato, ossia i casi di responsabilità colposa. In queste ipotesi potrebbe aversi una responsabilità per colpa del programmatore per difetto di programmazione, costruzione, utilizzo, manutenzione o funzionamento, nonostante si possa anche ipotizzare l'insussistenza di una responsabilità per negligenza, in quanto per l'operatore non appare prevedibile l'agire di un AI, dotato di capacità autonome di elaborazione delle informazioni. Ma si può anche giungere alla conclusione opposta, ritenendo che chi immetta nell'ambiente un AI, debba poter prevedere ogni tipo di danno da questo cagionato, anche in assenza di spiegazioni causali. Tuttavia, il riconoscimento di ampie responsabilità e un conseguente atteggiamento troppo cauto nella produzione di AI a causa della loro mancanza di controllabilità in via precauzionale, potrebbe limitare eccessivamente il ricorso ad AI e alle tecnologie più innovative. Considerata la specificità dei reati commessi dai sistemi di AI, alcuni Autori ipotizzano peraltro di introdurre "una nuova generazione di delitti". In questi termini Magro (2018), p. 2.

[62] Consulich (2018), p. 219.
In generale, in materia di intelligenze artificiali (AI), una parte della dottrina, riferendosi più genericamente al caso della responsabilità dei soggetti-persone fisiche per gli illeciti commessi dalle medesime AI, ha fatto riferimento a due ulteriori meccanismi imputativi: quello dell'autore mediato, la cui disciplina troverebbe applicazione quando il reato sia materialmente commesso da un "agente" innocente, penalmente non perseguibile; tuttavia, in questo caso, si potrebbe ribattere che l'art. 111 c.p. si rivolga solo alle persone. Altra ipotesi potrebbe essere quella del concorso anomalo di programmatori e utenti, penalmente responsabili del reato commesso dall'AI se tale reato sia la conseguenza

In particolare, con riferimento alla prima soluzione prospettabile, riferibile all'*actio libera in causa*, parte della dottrina ha evidenziato come, in questo caso, si tratterebbe di riscontrare una responsabilità in ogni comportamento che, pur privo di volontà antidoverosa, possa farsi risalire ad una precedente scelta libera e consapevole di agire. Al riguardo, secondo la dottrina, tale meccanismo ascrittivo, formalizzato all'art. 87 c.p., richiede una perfetta corrispondenza tra il reato commesso e quello programmato e, dunque, un nesso psichico tra fatto e autore piuttosto che una mera derivazione causale[63].

Tuttavia, sembrano sussistere due ostacoli all'applicazione dell'istituto dell'*actio libera in causa* rispetto a condotte di abuso di mercato ad opera di HFT. Si tratterebbe di un limite normativo, non essendo il meccanismo imputativo riferibile a qualsiasi esimente ma soltanto, ai sensi dell'art. 87 c.p., alla capacità di intendere e di volere; ogni ulteriore espansione determinerebbe quindi un'analogia in *malam partem*. Un limite soggettivo, dal momento che l'imputazione del fatto al soggetto presuppone una coincidenza tra il reato realizzato e il programma criminoso configurato *ex ante* dal reo, sulla base di una corrispondenza guidata da intenzionalità, elemento che mancherebbe nel caso delle operazioni autonomamente condotte dall'operatore algoritmico[64].

Considerate le insufficienze di tale soluzione, un'ulteriore strada da percorrere per poter stigmatizzare eventuali turbative del mercato riconducibili agli operatori algoritmici, potrebbe allora essere quella illustrata dalla disciplina della responsabilità degli enti, con particolare riferimento al modello imputativo di cui all'art. 8 d.lgs. n. 231/2001, in forza del quale è prevista la responsabilità della persona giuridica anche laddove alcun rimprovero possa essere mosso alla persona fisica. Al riguardo, la configurazione di un nuovo modello di colpevolezza *sui generis*, da intendersi in senso normativo e, dunque, concepita come "rimproverabilià" del soggetto, consentirebbe di prescindere, tutte le volte in cui l'illecito sia realizzato mediante HFT, dal nesso psichico tra fatto e autore e dall'integrazione dei requisiti di rappresentazione e volontà del fatto tipico.

Orbene, l'art. 8 del predetto decreto distingue due ipotesi, prevedendo la responsabilità dell'ente anche laddove il soggetto-persona fisica non sia imputabile o non sia stato identificato. Con specifico riferimento al caso in cui il *market abuse* sia veicolato dall'operare di un HFT, si potrebbero distinguere due casi; nel primo, in cui il programmatore o operatore fisico sia identificato ma non sia imputabile, potranno trovare applicazione gli artt. 6 e 7 del d.lgs. n. 231/2001; nel caso in cui invece l'operare dell'algoritmo non consenta di identificare il soggetto fisico, potrà trovare applicazione il predetto art. 8 del decreto. Invero, l'utilizzo improprio o abusivo dell'HFT può radicarsi nel contesto di una accettazione aziendale o di sfruttamento volontario della loro "propensione distorsiva del mercato", senza che la condotta specifica possa necessariamente ricondursi ad un soggetto-persona fisica precisamente individuato.

In altri termini, il reato commesso da soggetti carenti del dolo può, al verificarsi di certe condizioni, essere imputato ad una "colpa di organizzazione". In questi termini si esprime anche una parte della dottrina secondo cui, suggestivamente, l'art. 8 finirebbe dunque per svolgere "una funzione preventiva d'avanguardia proprio nei contesti più avvenieristici del reato economico, consentendo l'intervento penalistico rispetto alle ipotesi di irresponsabilità organizzata"[65]. La disposizione citata può in questo modo rappresentare un rimedio proprio nei casi in cui non sia possibile o risulti particolarmente difficoltoso imputare la responsabilità da reato ad un soggetto rispetto a fatti realizzati da operatori algoritmici, oltre a costituire altresì un referente normativo in relazione ad eventuali casi di danni causati dall'operare di tali meccanismi, espressione della generazione tecnologica più evoluta. Invero, in tali ipotesi, la presenza di modelli comportamentali e di corretta organizzazione, predisposti con finalità di prevenzione dei reati della specie di quelli verificatisi, consentirebbe, nel caso di negoziazioni compiute da HFT, di rendere autonomo l'accertamento della responsabilità dall'integrazione dei requisiti di rappresentazione e volontà del fatto tipico richiesti per le persone fisiche[66].

naturale o probabile di un loro comportamento illecito; in particolare, se programmatori o utenti abbiano programmato o utilizzato un AI per commettere un reato, ma l'AI abbia deviato il proprio comportamento commettendo un diverso reato, si potrebbe fare ricorso ad una particolare ipotesi di *aberratio delicti*, e in particolare alla figura del concorso anomalo nel reato, prevista dall'art. 116 c.p.

[63] Sul tema Cornacchia *et al.* (2007), p. 603; Fiandaca e Musco Enzo (2014), p. 361; Mantovani (2015), p. 649; Palazzo (2016), p. 434; Romano e Grasso (2012), pp. 29 ss.

[64] Consulich (2018), p. 219.

[65] Consulich (2018), p. 232.

[66] In questi termini l'innovativa ricostruzione di Consulich (2018), p. 232 che propone l'eventualità di ricorrere a tali meccanismi di imputazione della responsabilità anche rispetto a contesti avanguardistici come per esempio nell'ambito delle intelligenze artificiali. Si rinvia

Orbene, il riferimento all'art. 8 del d.lgs. n. 231/2001 quale possibile strumento che consenta di ascrivere profili di responsabilità ai soggetti-persone fisiche che abbiano impartito delle indicazioni o si siano avvantaggiati del ricorso agli HFT, potrebbe trovare un ostacolo in quell'orientamento dottrinale, oggi prevalente, secondo cui l'art. 8, nel consentire di prescindere dall'identificazione dell'autore fisico, ma non dalla commissione di un fatto di reato completo di tutti i suoi elementi oggettivi e soggettivi, assuma una valenza prettamente probatoria, non costituendo autonomamente un criterio imputativo di responsabilità[67]. In proposito infatti, come sottolineato da attenta dottrina, occorre distinguere tra mancata identificazione del soggetto responsabile e assenza di un fatto tipico di reato doloso, nella specie di manipolazione del mercato. In questo caso, infatti, si potrebbe incorrere nel pericolo di ascrivere la responsabilità per un reato doloso ad un soggetto, pur nell'impossibilità di individuare un qualsiasi colpevole e in assenza di un dolo quale coefficiente psichico reale.

Al riguardo, ragionando in un'ottica *de iure condendo*, potrebbero tuttavia altresì evidenziarsi le considerazioni proposte da una parte minoritaria della dottrina[68], secondo cui richiedere la verifica della commissione di un reato completo in tutti i suoi elementi soggettivi ed oggettivi rischierebbe di limitare eccessivamente la portata della disposizione stessa; a ciò si aggiunga che accogliendo tale impostazione si finirebbe per far venir meno la responsabilità dell'ente proprio nei casi in cui appaia maggiormente necessario intervenire nei suoi confronti, anche in ragione di una "disorganizzazione" interna tale da rendere difficoltosa l'individuazione del reo[69]. Inoltre, secondo alcuni Autori, proprio la mancata individuazione del soggetto "autore" del reato renderebbe oltremodo complesso accertare la sussistenza dell'illecito completo di tutti i suoi elementi costitutivi e, in particolare, di verificare se il soggetto fosse in possesso dell'elemento soggettivo richiesto ai fini dell'integrazione del reato[70]. Secondo tali tesi, pertanto, l'art. 8 consentirebbe di sanzionare la persona giuridica anche laddove difettino il dolo o la colpa del soggetto "autore" del reato.

6. La Direttiva n. 57/2014 e lo stato di adeguamento dell'ordinamento italiano alla normativa europea.

La rilevanza assunta dal settore del *market abuse*, lungi dall'essere limitata entro i confini della *domestic jurisdiction*, deve oggi necessariamente essere affrontata anche alla luce della normativa eurounitaria.

Invero, l'importanza degli interessi in gioco, di rilevanza sovranazionale, e le significative ricadute che la disciplina di settore assume, in grado di travalicare i confini nazionali dei singoli Stati, hanno suscitato l'interesse del legislatore europeo, il quale è intervenuto in materia, anche recentemente, introducendo tra le altre cose obblighi informativi e precisi requisiti organizzativi.

Al riguardo assume peculiare rilievo la cd. "direttiva abusi di mercato" n. 2014/57/UE, del 16 aprile 2014 (cd. MAD II, la quale approfondisce gli aspetti di rilievo penale del *market abuse*, con riferimento agli illeciti più gravi)[71] e il Regolamento UE sugli abusi di mercato, n.

anche a Bartoli (2016), pp. 1 ss.
Sul punto, inoltre, l'art. 16 del Regolamento UE n. 596/2014 prevede l'obbligo per i gestori del mercato e le imprese di investimento che gestiscono una sede di negoziazione di istituire e mantenere dispositivi, sistemi e procedure efficaci al fine di prevenire e individuare abusi di informazioni privilegiate, manipolazioni del mercato e tentativi di abuso di informazioni privilegiate e manipolazioni del mercato conformemente agli articoli 31 e 54 della Direttiva 2014/65/UE. In materia di responsabilità degli enti si rinvia a Militello (1998), pp. 367 ss.

[67] De Vero (2008), pp. 204-209; Pulitanò (2003), pp. 953 ss.

[68] Paliero (2003), pp. 19-20; Musco (2001), pp. 8 ss.

[69] Lasco *et al.* (2017), p. 127.

[70] Lottini (2007), pp. 2340 ss.

[71] Alla direttiva è demandata l'individuazione dello *standard* minimo di reazione punitiva (penale) che gli ordinamenti nazionali devono garantire, a fronte di violazioni della normativa regolamentare e, ad essa, è attribuito l'obiettivo dichiarato, assieme al MAR, di uniformare il trattamento amministrativo e penale, quest'ultimo riservato alle più gravi condotte integranti i reati di abuso di mercato, rafforzando di conseguenze le attività di prevenzione.
La direttiva UE, in altre parole, stabilisce le norme minime per l'applicazione delle sanzioni penali applicabili all'abuso di informazioni privilegiate, alla comunicazione illecita di informazioni privilegiate e alla manipolazione del mercato, al fine di assicurare l'integrità dei mercati finanziari all'interno dell'Unione e di rafforzare la protezione degli investitori e la fiducia in tali mercati.
La Direttiva invita inoltre gli Stati ad estendere la soglia di punibilità anche al tentativo di reato.

596/2014 (cd. MAR)[72], anch'esso del 16 aprile 2014 (che tuttavia riguarda piuttosto i profili amministrativi)[73], cui è stata data attuazione, nell'ordinamento italiano, con il d.lgs. 10 agosto 2018, n. 107, recante "Norme di adeguamento della normativa nazionale alle disposizioni del regolamento (UE) n. 596/2014", che tuttavia ribadisce, con poche e non significative varianti, prese di posizione sostenute in epoca risalente.

Inoltre, il 15 maggio 2014 il Consiglio UE ha approvato il cd. pacchetto MiFID II, composto dal Regolamento UE n. 600/2014 (MiFIR, sui mercati degli strumenti finanziari)[74] e dalla Direttiva 2014/65/UE[75], del 15 maggio 2014 (MiFID II, relativa ai mercati degli strumenti finanziari), integrata dal Regolamento n. 2017/578/UE e attuata in Italia con d.lgs. del 3 agosto 2017, n. 129, in vigore dal 3 gennaio 2018 (che tuttavia non ha apportato particolari modifiche al titolo V del T.U.F.), che tra le altre cose impone agli HFTr (oltre che ai gestori delle piattaforme di negoziazione) l'obbligo di predisporre adeguati sistemi di controllo interni[76]. Gli HFT e i *trader* che utilizzano algoritmi, inoltre, sono soggetti a numerosi obblighi informativi, al fine di consentire alle autorità competenti un più efficace monitoraggio del fenomeno[77].

La normativa si propone, in via generale, di garantire una maggiore trasparenza delle transazioni, rendere più efficace il funzionamento del mercato interno degli strumenti finanziari, tutelare gli investitori, rafforzarne la fiducia e assicurare che le autorità di vigilanza dispongano di poteri adeguati per svolgere i loro compiti.

La Direttiva MiFID II presta inoltre particolare attenzione alle imprese che effettuino negoziazioni mediante l'utilizzo di algoritmi, comprendendo ogni modalità di negoziazione in cui un algoritmo calcolato tramite computer determini automaticamente parametri individuali di ordini senza alcun intervento umano (considerando 59-68)[78].

In attuazione della Direttiva si attribuiscono inoltre alla CONSOB poteri di vigilanza con riguardo ai sistemi e ai controlli di cui devono dotarsi le banche e le imprese di investimento nella gestione di sedi di negoziazione, nonché in relazione all'attività di negoziazione algoritmica e ai partecipanti alle sedi di negoziazione.

[72] Tale Regolamento abroga la Direttiva 2003/6/CE e le Direttive 2003/124/UE, 2003/125/CE e 2004/72/CE. Il Regolamento UE n. 596/2014, integrato anche dal Regolamento UE 2016/522/UE, ha ad oggetto i profili amministrativi delle fattispecie di abuso di mercato, con la finalità dichiarata di garantire regole uniformi e chiarezza dei concetti di base, nonché un testo normativo unico.
Il Regolamento, infatti, che è entrato in vigore il 3 luglio 2016, istituisce il nuovo quadro normativo comune in materia di informazioni privilegiate, comunicazione illecita di informazioni privilegiate e manipolazione del mercato, nonché misure per prevenire gli abusi di mercato, per garantire l'integrità dei mercati finanziari dell'Unione ed accrescere la tutela degli investitori e, soprattutto, la fiducia in questi mercati.

[73] Per un approfondimento dei profili di adeguamento della disciplina nazionale alla normativa europea si rinvia a Gilotta e Raffaele (2018), pp. 83 ss.; Mucciarelli (2016), cit., pp. 193 ss.

[74] Il legislatore europeo "auspica" che la definizione di manipolazione del mercato fornisca esempi di strategie abusive specifiche che possano essere effettuate con qualsiasi strumento disponibile di scambio, inclusi quelli algoritmici e ad alta frequenza, al fine di adeguarsi alle più recenti forme di negoziazione.

[75] La Direttiva n. 65/2014 modifica la Direttiva 2002/92/CE e la Direttiva 2011/61/UE.
La direttiva, modificata dalla Direttiva 2016/1034/UE, è orientata ad adeguare la normativa nazionale alle disposizioni del regolamento UE n. 648/2012 (MiFIR), così come modificato dal regolamento UE 2016/1033. Il Regolamento UE n. 2016/1033 modifica a sua volta il Regolamento UE n. 600/2014 e il Regolamento UE n. 596/2014.
Il termine ultimo per il recepimento della Direttiva è fissato al 3 luglio 2016, mentre l'entrata in vigore di entrambi gli atti è stabilita al 3 gennaio 2017.

[76] Il d.lgs. n. 129/2017 apporta delle modifiche al d.lgs. n. 58/1998. In questa sede si segnala l'inserimento del comma 6 *quinquies* all'art. 1, il quale fornisce una definizione di negoziazione algoritmica.

[77] Sul tema, Consob, *http://www.consob.it/web/investor-education/mercati-finanziari*.

[78] Le predette imprese sono obbligate ad adottare sistemi e controlli del rischio volti ad assicurare che i sistemi di negoziazione siano flessibili, efficienti e siano soggetti a limiti e soglie idonei a prevenire l'erronea immissione di ordini o altre disfunzioni che potrebbero pregiudicare l'ordinato svolgimento delle negoziazioni sul mercato. Esse sono inoltre tenute ad assicurare che i loro sistemi non siano utilizzati per commettere abusi di mercato. Per quanto attiene alle negoziazioni ad alta frequenza e svolte attraverso algoritmi, la MiFID II impone particolari requisiti alle imprese di investimento che effettuano scambi "mediante l'utilizzo di algoritmi" (questo concetto è definito in maniera ampia per ricomprendere qualsiasi modalità di negoziazione che utilizzi un algoritmo ed in cui un algoritmo calcolato tramite computer determini automaticamente parametri individuali di ordini; per esempio, il momento di immissione dell'ordine, i tempi di esecuzione, il prezzo o la quantità dell'ordine senza alcun intervento umano). Le imprese che li usano saranno tenute ad adottare sistemi e controlli del rischio atti ad assicurare che i sistemi di negoziazione siano flessibili, efficienti e siano soggetti a limiti e soglie idonei a prevenire l'erronea immissione di ordini o altre disfunzioni che potrebbero pregiudicare l'ordinato svolgimento delle contrattazioni sul mercato. Esse sono inoltre tenute ad assicurare che i loro sistemi non siano utilizzati per commettere abusi di mercato. Inoltre, la MiFID II imporrà alle imprese di investimento di comunicare all'autorità di vigilanza dello Stato di origine e alle sedi di mercato l'utilizzo di strategie di negoziazione tramite algoritmi. Le autorità competenti avranno poi facoltà di richiedere ulteriori informazioni circa le strategie, i parametri e i limiti di scambio, e le modalità di controllo dei rischi che l'impresa ha adottato. Con riferimento agli strumenti *equity*, gli operatori dei mercati regolamentati, MTF e OTF saranno soggetti a requisiti di trasparenza pre-negoziazione. Essi dovranno pubblicare i prezzi di offerta e di vendita, le informazioni sulla domanda, i prezzi esposti sui loro sistemi e le indicazioni di interesse cui può esser dato corso su base continuativa durante il normale orario di negoziazione. Tale ricostruzione dei contenuti della Direttiva è rinvenibile nel dossier della Consob, Mercati degli strumenti finanziari, maggio 2017, disponibile all'indirizzo *http://www.dirittobancario.it/sites/default/files/allegati/mercati_degli_strumenti_finanziari.pdf*.

Gli strumenti normativi indicati sono i primi che, a livello europeo, affrontano il tema del *trading* ad alta frequenza, al fine di fornire una regolamentazione ad una materia tanto centrale quanto complessa.

7. Conclusioni.

Esaminando taluni aspetti problematici con i quali la materia del *market abuse* è oggi chiamata a confrontarsi rileva, in conclusione, la difficoltà di ipotizzare fattispecie tipiche e tassative laddove gli operatori finanziari si avvalgano di HFT, trattandosi di strumenti di negoziazione in grado di reagire alle diverse variabili contingenti e capaci dunque di evolversi continuamente in relazione al contesto in cui operano[79]. Difficile appare altresì l'individuazione dello specifico bene giuridico tutelato, nonché la ricostruzione dell'elemento soggettivo (anche nella forma del dolo eventuale) e di una eventuale posizione di garanzia. Ancora, risulta poco agevole identificare il soggetto al quale imputare i profili di responsabilità (il programmatore, l'utilizzatore o l'intermediario), nonché ricostruire i meccanismi di imputazione di responsabilità.

Anche con riferimento all'attuazione della normativa sovranazionale, il sistema italiano presenta taluni profili problematici. Tra questi lo scostamento dalle prescrizioni europee (direttive e regolamenti), l'omessa criminalizzazione dell'*insider* secondario e, in generale, il mancato coordinamento della normativa nazionale rispetto agli strumenti normativi europei. Su quest'ultimo punto, in particolare, si rilevano talune questioni in relazione alla definizione di "informazione privilegiata", ora dettata dalla lettera *b-ter)* dell'art. 180, comma primo, attraverso il rinvio all'art. 7 del Regolamento UE n. 596/2014; considerata la corrispondente abrogazione del previgente art. 181 T.U.F. (*ex* art. 4, comma quarto, d.lgs. n. 107/2018); infatti, la nuova descrizione di una delle nozioni di maggior rilievo nella disciplina del *market abuse* finisce per presentare contenuti non sovrapponibili a quelli della disposizione abrogata e non sempre coordinati con i contenuti del T.U.F.

Al riguardo, il d.lgs. n. 107/2018 avrebbe potuto contribuire ad un'attuazione effettiva della disciplina dell'UE (e in particolare della Direttiva 57/2014/UE).

Tuttavia il decreto si limita ad apportare poche e non significative modifiche[80].

In proposito, la crescente presenza di operatori algoritmici sul mercato richiederebbe forse la predisposizione di una normativa specificamente diretta a regolare la responsabilità derivante dall'impiego di tale tipologia di strumenti e a disciplinarne l'operatività[81], muovendo

[79] Altri problemi sono inoltre posti dal carattere transnazionale che permea la materia, accentuato dal ricorso al sistema della *delocalization*.

[80] Mucciarelli (2018b), pp. 3 ss. In generale si segnala che il percorso di attuazione della Direttiva 2014/57/UE e del Regolamento UE 596/2014 non è stato privo di ostacoli. I suggerimenti del Parlamento infatti non vengono inizialmente colti dal Governo, come emerge dalla lettura della l. n. 163/2017, recante Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016 – 2017. Sembra dunque che il Governo non reputi necessario un adeguamento del comparto penale della normativa interna contenuta nel d.lgs. n. 58/1998 (T.U.F.). Sul punto, nella Relazione illustrativa dello Schema di disegno di legge recante la Delega al Governo per il recepimento delle direttive europee – Legge di delegazione europea 2016 (poi divenuto l. n. 163/2017) si legge che "per quanto riguarda le sanzioni penali e amministrative pecuniarie previste rispettivamente dal regolamento (UE) n. 596/2014 e dalla Direttiva 2014/57/UE, l'attuale relativa disciplina sanzionatoria di riferimento è contenuta nella parte V del TUF. Nell'ordinamento interno, le condotte dolose previste dalla direttiva risultano già oggetto di previsione sanzionatoria". Ai sensi dell'art. 8 della l. n. 163/2017 non si rintraccia peraltro alcun riferimento alla Direttiva MAD II. Sul tema anche Basile (2016), cit., pp. 272-282; Basile (2015), p. 12-14.

[81] Sul tema "al fine di individuare talune possibili strategie di prevenzione e repressione del fenomeno del *market abuse*, oggi accentuato e reso più agevole dalla rapida diffusione degli HFT, potrebbero in primo luogo introdursi taluni controlli integrativi; si pensi, per esempio, all'introduzione di una imposizione dell'obbligo, in capo agli operatori algoritmici, di notificare alle autorità di controllo le caratteristiche degli algoritmi adottati e i relativi sistemi di gestione del rischio. Ulteriore strumento di controllo si ravviserebbe nei cd. "*circuit breakers*", ossia meccanismi per limitare o interrompere il *trading* al verificarsi di determinate condizioni. I *circuit breakers* richiedono comunque un'attenta modulazione al fine di non rallentare il processo di *price discovery* e di non creare i presupposti per un aumento dell'incertezza e della volatilità al momento della riapertura delle contrattazioni. Alcune evidenze empiriche, inoltre, mostrano come i *circuit breakers* abbiano una sorta di "potere magnetico" in base al quale i *traders*, se conoscono la soglia (*trigger*) che determina l'attivazione del meccanismo di interruzione, cominciano a negoziare più velocemente quanto più ci si avvicina a tale soglia, in modo da chiudere le proprie posizioni prima dell'interruzione. In aggiunta, per contrastare il fenomeno negativo della "*ghost liquidity*", potrebbero definirsi sia un tempo minimo di permanenza sul *book* dei singoli ordini, sia il limite massimo al rapporto tra ordini immessi ed ordini eseguiti (OTR): di conseguenza, si otterrebbe una mitigazione degli effetti distorsivi sulla reale profondità del *book*, causati dalla pratica dello "*stuffing*". Infine, una attenta regolamentazione della fornitura di servizi che permettono agli operatori di ridurre il tempo di *latency* (ad esempio, i servizi di *co–location*) è tra le misure ritenute utili a salvaguardare non solo l'equo accesso ai mercati, l'ordinato svolgimento delle negoziazioni, l'efficiente esecuzione degli ordini e l'integrità del mercato, ma anche a garantire che la robustezza e la velocità dei controlli sulle attività di negoziazione siano al passo con la velocità operativa e i volumi fatti registrare dagli HFTr. A tal fine, l'operatore che si avvale dei servizi di *co–location* ovvero di *proximity hosting* potrebbe essere segnalato alle sedi di negoziazione attraverso specifiche modalità di "segregazione" (ad es. *flag* degli ordini e delle transazioni) e sottoposto

per esempio, in materia di reato di abuso di informazioni privilegiate, "dal commiato da una nozione onnicomprensiva di investitore ragionevole, che dunque dovrebbe rimanere applicabile al solo ambito degli operatori fisici, nonché dalla dissociazione tra azione di mercato e informazione finanziaria, in considerazione della capacità dell'HFT di 'scindere' l'operazione dall'informazione. Inoltre, con riferimento alla rilevanza delle informazioni privilegiate considerate rispetto all'investitore ragionevole, si potrebbe ricomporre la dicotomia tra investitore ragionevole e irrazionale attraverso un nuovo schema, quello dell' "investitore senza qualità", strutturalmente più informato di un investitore occasionale ed irrazionale, ma certo non in grado di dominare la grande mole di dati che riceve; sempre più veloce nelle proprie decisioni di investimento grazie ad un crescente supporto tecnologico, tale operatore non è immune da pulsioni imitative non meditate. Tali soggetti sono troppo eterogenei tra loro per obiettivi perseguiti, conoscenze iniziali e competenze specifiche per comporre una figura di sintesi cui parametrare le qualità dell'*informazione privilegiata*[82]".

Dal punto di vista del reato di "abuso di informazioni privilegiate", si pone dunque il problema di ricostruire il concetto di investitore ragionevole ed informazione privilegiata e, in generale, di adattare le fattispecie oggi esistenti in materia di *market abuse* al nuovo volto assunto dai mercati finanziari, interessati dall'evoluzione tecnologica.

Per quanto attiene al reato di manipolazione del mercato, occorre invece ricostruire i profili di responsabilità penale; tale operazione, anche laddove consenta di individuare il soggetto cui attribuire la responsabilità e il criterio di imputazione, può tuttavia comportare altresì delle criticità in sede probatoria, anche con riferimento alla ricostruzione e all'accertamento del fatto tipico.

Inoltre, appare auspicabile che la definizione di manipolazione del mercato fornisca esempi di strategie abusive specifiche che possano essere effettuate con qualsiasi strumento disponibile di negoziazione, incluse le negoziazioni algoritmiche e quelle ad alta frequenza, come già previsto ai sensi del Regolamento UE n. 596/201[83].

Inoltre, ci si deve chiedere se a fronte di una normativa generale dettata in materia di regolamentazione degli strumenti finanziari e degli abusi di mercato, quali la Direttiva MiFID II e il Regolamento MAR, si possa considerare esaustivamente disciplinato il "fenomeno HFT".

In questi termini sembra potersi riflettere in merito alle difficoltà scaturite da una disciplina che, seppur prevedendo specifici strumenti di controllo in materia, inserisce la fattispecie in parola in categorie normative già esistenti e predeterminate, riferibili a condotte originariamente riconducibili al solo "ecosistema dell'essere umano"[84].

Come ha segnalato la Consob, la crescente diffusione dell'HFT può destabilizzare i mercati, incidere sulla volatività e sulla liquidità dei titoli, amplificare movimenti anomali dei prezzi e, più in generale, può avere ripercussioni rilevanti su interi settori economici e, in definitiva, sull'integrità dei mercati. Da qui la necessità che il legislatore italiano riformi la materia in modo organico, tenendo conto delle indicazioni europee e conciliando la necessità di una tutela adeguata al nuovo volto assunto dal *market abuse* con il rispetto degli irrinunciabili principi del diritto penale, quali i principi di legalità, offensività, proporzionalità e personalità della responsabilità penale.

a controlli periodici effettuati da unità indipendenti"; in questi termini v. *http://www.giurisprudenzapenale.com/wp-content/uploads/2017/10/Market-Abuse-e-Trading-ad-alta-frequenza.pdf*.

[82] Consulich (2018), p. 217; Consulich e Mucciarelli (2016), cit., pp. 179 ss.; sul tema anche Miedico (2017), p. 326.

[83] Ai sensi dell'art. 8 del Regolamento UE n. 596/2014 sono indicate alcune operazioni che possono essere considerate, tra le altre, manipolazione del mercato: a) la condotta di una o più persone che agiscono in collaborazione per acquisire una posizione dominante sull'offerta o sulla domanda di uno strumento finanziario, di contratti a pronti su merci collegati o di un prodotto oggetto d'asta sulla base di quote di emissioni che abbia, o è probabile che abbia, l'effetto di fissare, direttamente o indirettamente, i prezzi di acquisto o di vendita o ponga in atto, o è probabile che lo faccia, altre condizioni commerciali non corrette; b) l'acquisto o la vendita di strumenti finanziari all'apertura o alla chiusura del mercato, con l'effetto o il probabile effetto di fuorviare gli investitori che agiscono sulla base dei prezzi esposti, compresi i prezzi di apertura e di chiusura; c) l'inoltro di ordini in una sede di negoziazione, comprese le relative cancellazioni o modifiche, con ogni mezzo disponibile di negoziazione, anche attraverso mezzi elettronici, come le strategie di negoziazione algoritmiche e ad alta frequenza, e che esercita uno degli effetti di cui al paragrafo 1, lettere a) o b), in quanto: 1) interrompe o ritarda, o è probabile che interrompa o ritardi, il funzionamento del sistema di negoziazione della sede di negoziazione; 2) rende più difficile per gli altri gestori individuare gli ordini autentici sul sistema di negoziazione della sede di negoziazione, o è probabile che lo faccia, anche emettendo ordini che risultino in un sovraccarico o in una destabilizzazione del book di negoziazione (*order book*) degli ordini; 3) oppure crea, o è probabile che crei, un segnale falso o fuorviante in merito all'offerta, alla domanda o al prezzo di uno strumento finanziario, in particolare emettendo ordini per avviare o intensificare una tendenza. 2.

[84] Sul tema v. anche *http://www.giurisprudenzapenale.com/wp-content/uploads/2017/10/Market-Abuse-e-Trading-ad-alta-frequenza.pdf*.

Bibliografia

Antolisei, Francesco (2000): *Manuale di diritto penale. Parte Speciale*, Vol. II, (Milano, Giuffré), pp. 525 ss.

Alvaro, Simone e Ventoruzzo, Marco (2016): "High-Frequency Trading: note per una discussione", in *Banca impresa società*, n. 3, pp. 417 ss.

Arenaccio, Marta, Camiciotti, Giorgio, Zaghini, Giuseppe (2016): *La nuova disciplina degli abusi di mercato. Verso la Capital market Union*, (Roma, Ecra), p. 53

Barrales, Edgar Ortega (2012): "Lessons from the flash crash, for the regulation of high frequency traders", in *Fordham Journal Corporate & Financial Law*, (Berkeley, Berkeley Electronic Press), pp. 1199 ss.

Bartoli Roberto (2016): "Alla ricerca di una coerenza perduta, o forse mai esistita", in *www.penalecontemporaneo.it*, 10 marzo 2016, pp. 1 ss.

Bartulli, Armando (1992): "Profili penalistici dell'insider trading", in Rabitti Bedogni Carla (editor): *Il dovere di riservatezza del mercato finanziario*, (Milano, Giuffré), pp. 163 ss.

Basile, Enrico (2015): "Verso la riforma della disciplina italiana del market abuse: la legge-delega per il recepimento della direttiva 57/2014/UE", in *Legisl. pen.*, 10 dicembre 2015, p. 12-14

Basile, Enrico (2017): "Una nuova occasione (mancata) per riformare il comparto penalistico degli abusi di mercato? Lo schema del d.d.l. di delegazione europea 2016", in *Dir. pen. cont.*, n. 5, pp. 271-282

Caivano, Valeria, Ciccarelli, Salvatore, Di Stefano, Giovanna, Fratini, Marco, Gasparri, Giorgio, Giliberti, Monica, Linciano, Nadia, Tarola, Isadora (2012): "Il trading ad alta frequenza. Caratteristiche, effetti, questioni di *policy*", in *www.consob.it*, 5 dicembre, pp. 7-18.

Canestrari Stefano, Cornacchia Luigi, De Simone Giulio (2007): *Manuale di diritto penale. Parte gen.*, (Bologna, Il Mulino), p. 603

Carriero, Giuseppe (1992): *Informazione, mercato, buona fede: il cosiddetto insider trading*, (Milano, Giuffré), pp. 2 ss.

Consob: "Mercati finanziari", consultabile all'indirizzo *http://www.consob.it/web/investor-education/mercati-finanziari*

Consulich, Federico e Mucciarelli, Francesco (2016): "Informazione e tutela penale dei mercati finanziari nello specchio della normativa eurounitaria sugli abusi di mercato", in *Le Società*, n. 2, pp. 179 ss.

Consulich, Federico (2018): "Il nastro di möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso di mercato", in *Banca borsa titoli di credito*, n. 2, p. 196

De Vero, Giancarlo (2008): *La responsabilità penale delle persone giuridiche, IV, Trattato di diritto penale*. *Parte generale*, (Milano, Giuffré), p. 204-209

European Security and market abuse (ESMA): "Economic Report. High-frequency trading activity" in EU equity markets, n. 1/2014, p. 4

Falcinelli Daniela (2018): "Il dolo in cerca di una direzione penaleIl contributo della scienzarobotica ad una teoriadelle decisioni umane", in *Arch. pen.*, n. 1/2018, p. 5

Fiandaca Giovanni e Musco Enzo (2014): *Diritto penale, Parte gen.*, (Bologna, Giappichelli), p. 361

Giavazzi, Stefania (2009): "L'abuso di informazioni privilegiate", in Cerqua, Luigi Domenico (editor): *Diritto penale delle società. Profili sostanziali e processuali,* Vol. I, (Padova, Cedam), pp. 801 ss.

Gilotta, Sergio e Raffaele, Federico (2018): "Informazione privilegiata e "processi prolungati" dopo la Market Abuse Regulation", in *Rivista delle Società*, n. 1, pp. 83 ss.

Gomber, Peter, Arndt, Björn, Lutat, Marco, Uhle, Tim (2011): *High-Frequency Trading, Goethe Universität Technical Report*, commissioned by Deutsche Börse

Grosso, Carlo Federico, Pelissero, Marco, Petrini, Davide, Pisa, Paolo (2017): *Manuale di diritto penale, Parte generale*, (Milano, Giuffré), p. 332

Hu, Henry (2012): "Too Complex to Depict? Innovation, "Pure information", the SEC Disclosure Paradigm", in *Tex. L. Rev.*, pp. 1705 ss.

Lasco, Giuseppe, Loria, Velia, Morgante, Mariavittoria, *Enti e responsabilità da reato. Commento al D.Lgs. 8 giugno 2001, n. 231*, (Torino, Giappichelli), p. 127

Lottini, Riccardo (2007): "Responsabilità delle persone giuridiche" in Palazzo, Francesco e Paliero, Carlo Enrico, (eds.) *Commento breve alle leggi penali complementari, II*, (Padova, Cedam), pp. 2340 ss.

Magro, Maria Beatrice (2014): in Provolo Debora, Riondato Silvio, Yenisey Feridun, *Genetics, Robotics, Law, Punishment*, (Padova, Padova University Press), p. 514

Magro, Maria Beatrice (2018): "A.I.: la responsabilità penale per la progettazione, la costruzione e l'uso dei robot", in *Quot. giur.*, 12 giugno 2018, p. 2

Manno, Marco Andrea (2012): *Profili penale dell'insider trading*, (Milano, Giuffrè), pp. 1 ss.

Mantovani Ferrando (2015), *Diritto penale. Parte gen.*, (Padova, Cedam), p. 649;

McGowan, Michael (2010): "The Rise of Computerized High-Frequency Trading: Use and Controversy", in *Duke Law & Technology Review*, pp. 1 ss.

Miedico Melissa (2017): "Gli abusi di mercato", in Alessandri Alberto (editor), *Reati in materia economica*, (Torino, Giappichelli), p. 326

Militello Vincenzo (1998): "Attività del gruppo e comportamenti illeciti: ilgruppo come fattore criminogeno", in *Riv.trim.pen.ec.*, pp. 367

Mucciarelli, Francesco (2000): "L'insider trading nella nuova disciplina del D.Lgs. 58/98", in *Riv. trim. dir. pen. ec.,* pp. 932 ss.

Mucciarelli, Francesco (2002): "Aggiotaggio", in Alessandri Alberto (editor): *Il nuovo diritto penale delle società*, (Assago, Ipsoa), pp. 431 ss.

Mucciarelli, Francesco (2005): "L'abuso di informazioni privilegiate: delitto e illecito amministrativo", in *Dir. pen. e proc.*, pp. 1472 ss.

Mucciarelli, Francesco (2016): "L'insider trading nella rinnovata disciplina UE sugli abusi di mercato", in *Le società*, n. 2, pp. 193 ss.

Mucciarelli, Francesco (2018a): "Riforma penalistica del market abuse: l'attesa continua", in *Dir. pen. e proc.*, n. 1, pp. 5 ss.

Mucciarelli, Francesco (2018b): "Gli abusi di mercato riformati e le persistenti criticità di una tormentata disciplina. Osservazioni a prima lettura sul decreto legislativo 10 agosto 2018, n. 107", in *Dir. pen. cont.*, 10 ottobre 2018, pp. 3 ss.

Musco, Enzo (2001), "Le imprese a scuola di responsabilità tra pene pecuniarie e interdizioni", *Dir. e giustizia*, pp. 8 ss.

Musco, Enzo (2007): *I nuovi reati societari*, Giuffré, pp. 282 ss.

Padovani, Tullio (1995): "Diritto penale della prevenzione e mercato finanziario", in *Riv. it. dir. pr. pen*., p. 641

Palazzo, Francesco (2016), *Corso di diritto penale. Parte Generale*, (Torino, Giappichelli), p. 434

Paliero, Carlo Enrico (2003), "La responsabilità penale della persona giuridica nell'ordinamento italiano: Profili sistematici", in Palazzo, Francesco (editor): *Societas puniri potest, la responsabilità da reato degli enti collettivi*, (Padova, Cedam), pp. 19-20.

Preziosi, Stefano (2008): *La manipolazione di mercato nella cornice dell'ordinamento comunitario e del diritto penale italiano*, (Bari, Cacucci ed.)

Pulitanò, Domenico (2003): "Responsabilità amministrativa dipendente da reato delle persone giuridiche", *Enc. Dir*., XXVII, pp. 953 ss.

Puorro, Alfonso (2013): "High Frequency Trading: una panoramica", in *Banca d'Italia, Questioni di economia e finanza*, reperibile sul sito *www.bancaditalia.it*, pp. 10 ss.

Quirici, Maria Cristina (2006): "Tratti Evolutivi della disciplina in tema di abusi di mercato alla luce del recente recepimento della direttiva 2003/6/CE", in *Studi e Note di Economia*, n. 2, pp. 111 ss.

Romano e Grasso (2012), *Commentario del codice penale*, Sub *art. 87*, II, (Milano, Giuffré), pp. 29 ss.

Scopino, Gregory (2015): "Preparing Financial Regulation for the Second Machine Age: The Need for Oversight of Digital Intermediaries in the Futures Markets", in *Colum. Bus. L. Rev.*, p. 458

Seminara, Sergio (2000): "La tutela penale del mercato finanziario", in Pedrazzi Cesare – Alessandri Alberto – Foffani Luigi – Seminara Sergio – Spagnolo Giuseppe (eds.): *Manuale di diritto penale dell'impresa*, (Bologna, Zanichelli), p. 514

Sgubbi, Filippo (2008): "Riflessioni introduttive", in Sgubbi, Filippo, Fondaroli, Désirée, Tripodi, Andrea Francesco (eds.): *Diritto penale del mercato finanziario*, (Padova, Cedam), pp. 3 ss.

Strampelli, Giovanni (2014): "L'informazione societaria a quindici anni dal T.U.F.: profili evolutivi e problem", in *Riv. soc*., pp. 991 ss.

Yadav, Yesha (2014): "Beyond Efficiency in Securities Regulation", reperibile sul sito *http://ssrn.com/abstract=2400527*, p. 37.

Gli strumenti di prevenzione nazionali ed europei in materia di valute virtuali e riciclaggio

Los instrumentos de prevención nacional y europeos en materia de monedas virtuales y lavado de activos

Domestic and European Preventative Instruments Concerning Virtual Currencies and Money Laundering

Cristina Ingrao
Dottoranda in "Pluralismi giuridici. Prospettive antiche e attuali" presso l'Università di Palermo
cristina.ingrao@unipa.it

Riciclaggio | Lavado de activos | Money Laundering

Abstracts

L'utilizzo crescente di monete virtuali solleva da tempo dibattiti circa il nesso esistente fra le stesse e il mondo del crimine, sul sospetto che tale nuovo strumento di pagamento si presti ad essere sfruttato dalla criminalità come sistema finanziario alternativo, a fini di riciclaggio, in assenza di controlli da parte delle Autorità. Proprio a fronte di tali rischi di recente sono stati adottati, in ambito sovranazionale e nazionale, innovativi strumenti normativi di carattere preventivo; il tema del riciclaggio e delle valute virtuali, infatti, si presta ad essere affrontato, oltre in prospettiva repressiva, anche in prospettiva preventiva. Con il presente lavoro si intende procedere proprio all'analisi degli strumenti preventivi adottati in materia, per individuare quelli più idonei al contrasto di tali nuove pratiche, attraverso lo studio della normativa sovranazionale di settore e al confronto fra la stessa e quella italiana, per giungere ad un'analisi sulla situazione attuale e sulle prospettive sul tema.

La utilización creciente de monedas virtuales plantea desde hace tiempo debates acerca del nexo existente entre las mismas y el mundo del crimen. En efecto, existe la sospecha de que estos nuevos instrumentos de pago sean aprovechados por las organizaciones criminales como sistema financiero alternativo a fines de lavado de activos, debido a la ausencia de controles por parte de la autoridad. Para hacer frente a tales riesgos, recientemente han sido adoptados, tanto a nivel nacional como internacional, instrumentos normativos de carácter preventivo. El presente trabajo tiene por objeto analizar los instrumentos preventivos nacionales y europeos adoptados en la materia, a fin de individuar aquellos más idóneos en el combate de aquellas prácticas.

The increasing use of virtual currencies has posed questions over the time about links with criminal activities, i.e. the possibility of becoming an alternative financial instrument for money laundering purposes in the lack of supervision by the authorities. Recently several preventative measures have been adopted both at the domestic and the supranational level: the risk of money laundering through virtual currencies can be indeed managed also from a preventative perspective. This paper aims to analyse the preventative instruments, in order to identify the most apt to combat unlawful practices, by studying the supranational legislation and comparing it with the Italian one, to analyse the whole scenario and the future developments.

Sommario

1. Premessa. Valute virtuali e riciclaggio: strumenti di prevenzione.

Il tema del riciclaggio e delle valute virtuali (o criptovalute) necessita di essere affrontato, oltre che in prospettiva repressiva, anche in prospettiva preventiva, alla luce dei recenti interventi legislativi che si sono susseguiti in materia e che lasciano numerosi dubbi su una regolamentazione efficace della stessa.

Lo scopo delle attività di prevenzione è, in generale, quello di intercettare anticipatamente le infiltrazioni criminali nel sistema economico legale: in tale attività complessa, una particolare attenzione viene prestata ai mezzi di pagamento, quali strumenti che possono essere impiegati nell'esecuzione delle transazioni finanziarie per finalità di riciclaggio o finanziamento del terrorismo; il riferimento è, per ciò che a noi interessa, alle valute virtuali. L'utilizzo crescente di monete virtuali, infatti, solleva da tempo discussioni circa il nesso esistente fra le stesse e il mondo del crimine, sul sospetto che tale nuovo strumento di pagamento si presti ad essere sfruttato dalla criminalità al fine trasferire, nascondere e ripulire i proventi di attività illecite, in assenza di controlli da parte delle Autorità.

Del resto, il pericolo che la criptovaluta divenga lo strumento principale per attività di riciclaggio è insito nelle sue caratteristiche, essendo la stessa idonea per natura a dissimulare il valore oggetto del suo trasferimento nella vastità della realtà virtuale. In particolare, la valuta virtuale cumula in sé i vantaggi della moneta elettronica e quelli del contante, in quanto come una banconota è anonimo, e pertanto non richiede la notorietà delle identità delle controparti e della causale di pagamento; ma, essendo digitale, consente trasferimenti per qualunque importo, da pagamenti irrisori al regolamento di traffici commerciali internazionali.

Tecnicamente le criptovalute permettono di effettuare pagamenti *on line* in maniera sicura grazie a tecnologie di tipo *peer to peer* (p2p)[1], che si fondano su "catene di blocchi" (c.d. *blockchain*), costituiti da computer di utenti disseminati in tutto il mondo su cui vengono eseguiti appositi programmi che svolgono funzioni di portamonete (*wallet*).[2]

A fronte dei rischi connessi a tale sistema finanziario alternativo, come accennato, sono stati adottati, in ambito sovranazionale e nazionale, innovativi strumenti normativi di carattere preventivo.

Il riferimento è, a livello di Unione Europea, alle recenti Direttive antiriciclaggio n. 843/2018/UE e n. 849/2015/UE, relative alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo. Come si avrà modo di precisare meglio in seguito, la Direttiva del 2015, c.d. IV Direttiva antiriciclaggio, è stata oggetto di modifica e integrazione da parte della Direttiva del 2018, c.d. V Direttiva antiriciclaggio.

Quanto alla normativa nazionale, occorre considerare, in particolare, il D.lgs. n. 90/2017, intitolato "*Attuazione della Direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle Direttive 2005/60/CE e 2006/70/CE e attuazione del Regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il Regolamento (CE) n. 1781/2006*", attraverso cui si è inteso implementare, a livello interno, la Direttiva antiriciclaggio del 2015.

Ciò premesso, con il presente lavoro si intende procedere all'analisi degli strumenti normativi a carattere preventivo che negli ultimi anni si sono occupati delle nuove modalità di realizzazione del riciclaggio effettuato attraverso l'uso di valute virtuali, al fine di individuare gli strumenti più idonei al contrasto di tali nuove pratiche. Si procederà, pertanto, allo studio della normativa sovranazionale di settore più recente, cui si è fatto cenno, e al confronto fra la stessa e la normativa italiana, che si è mostrata, nel campo delle valute virtuali, anticipatrice e

[1] L'espressione "*peer to peer*" va intesa nel senso di "pari a pari", che identifica un rapporto *inter pares*.
[2] Majorana (2018), pp. 630-631.

innovatrice, per giungere a svolgere alcune considerazioni sullo stato della situazione attuale e sulle prospettive in materia.

2. La normativa di riferimento.

2.1. *La Direttiva n. 849/2015/UE e l'assenza di previsioni in materia di criptovalute.*

Punto di partenza dell'analisi degli strumenti preventivi adottati al livello sovranazionale è la Direttiva n. 849/2015/UE, che ha costituito negli anni scorsi il principale strumento giuridico europeo per la prevenzione dell'uso del sistema finanziario dell'Unione Europea a fini di riciclaggio di denaro e finanziamento del terrorismo, mediante la definizione di un quadro giuridico efficiente e completo per il contrasto della raccolta di beni o di denaro a scopi terroristici.[3]

La Direttiva, in particolare, ha inteso sia rafforzare la normativa dell'Unione Europea in tema di riciclaggio e di finanziamento al terrorismo, sia garantirne la coerenza con gli *standard* globali stabiliti nelle Raccomandazioni internazionali adottate dal gruppo di azione finanziaria internazionale (GAFI) del 2012.

Si compone di VII Capi che afferiscono alle disposizioni generali e finali, nonché a macro categorie di interesse, quali l'adeguata verifica della clientela o le disposizioni per le Autorità di Vigilanza[4], tutte funzionali al contrasto al riciclaggio e al finanziamento del terrorismo; tuttavia, come si avrà modo di approfondire in seguito, non contiene alcun riferimento al nuovo fenomeno delle valute virtuali e del loro utilizzo a fini di riciclaggio.

Suo tratto caratterizzante è senza dubbio l'estensione e la razionalizzazione del principio dell'approccio basato sul rischio (*risk based approach*)[5] che, a ben vedere, contraddistingueva già la c.d. III Direttiva antiriciclaggio, n. 60/2005/CE.[6]

Tale approccio è finalizzato a valutare i rischi di riciclaggio e finanziamento al terrorismo insiti nell'esercizio delle attività, finanziarie e professionali, svolte dai destinatari della normativa. Deve guidare, da un lato, il comportamento dei soggetti obbligati e, dall'altro, l'azione di controllo a cui sono chiamate le autorità[7]; la prevenzione del riciclaggio e del finanziamento del terrorismo, infatti, deve necessariamente passare da una piena responsabilizzazione dei soggetti obbligati rispetto alle procedure necessarie per mappare e intercettare il rischio insito nella pratica quotidiana della loro attività professionale.[8]

Oltre all'approccio basato sul rischio la IV Direttiva prevede degli strumenti specifici di contrasto al riciclaggio e al finanziamento al terrorismo, che rappresentano le macro aree cui si è fatto cenno in apertura del paragrafo. Si tratta di mezzi di intervento che consistono nell'assoggettamento agli obblighi di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo dei prodotti di moneta elettronica, in presenza del superamento di determinate soglie economiche (art. 12), nel rafforzamento delle misure di adeguata verifica della clientela (artt. 18 e ss.), nella previsione di un nuovo registro centralizzato di informazioni riguardanti la proprietà effettiva delle società e dei *trust* (art. 30), nel rafforzamento degli obblighi di segnalazione (artt. 32 e ss.) a carico dei soggetti obbligati e nel rafforzamento degli obblighi di conservazione (art. 40).

L'ultima parte della IV Direttiva è, infine, riservata alle sanzioni (artt. 58 e ss.), in previsione di una loro armonizzazione a livello nazionale. Ciò in quanto tradizionalmente gli Stati membri dispongono di differenti sanzioni e misure amministrative per le violazioni delle disposizioni di natura preventiva e tale diversità nazionale può pregiudicare gli sforzi compiuti

[3] Rossi (2018), p. 26.
[4] Salvini (2016), pp. 154-155.
[5] Il *risk based approach* è espressamente previsto dagli artt. 6, 7 e 8 della IV Direttiva, rispettivamente a livello europeo, nazionale e a livello dei soggetti obbligati.
[6] Relativa anch'essa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.
[7] Rossi (2018), p. 26.
[8] Relazione sull'attività di prevenzione del riciclaggio e del finanziamento del terrorismo e rapporto annuale sull'attività svolta dall'Unità di Informazione Finanziaria (UIF) della Banca d'Italia, in *https://www.senato.it/service/PDF/PDFServer/DF/325614.pdf* (2015), pp. 1 ss.

per contrastare il riciclaggio e il finanziamento del terrorismo a livello sovranazionale.

Dall'esposizione svolta dei tratti essenziali della Direttiva del 2015 emerge la mancata estensione agli operatori del settore criptovalutario dell'applicazione della normativa antiriciclaggio.

Tale mancata previsione si è rivelata fallace.

Gli attacchi terroristici che hanno interessato il nord Europa negli ultimi anni, infatti, hanno evidenziato l'emergere di nuove tendenze per quanto attiene alle modalità con cui i gruppi terroristici finanziano e svolgono le proprie operazioni. Alcuni servizi basati sulle moderne tecnologie, come le monete virtuali, in particolare, sono divenuti sempre più popolari come sistemi finanziari alternativi, posto che a lungo sono rimasti al di fuori dell'ambito di applicazione del diritto europeo o hanno beneficiato di deroghe all'applicazione di obblighi giuridici che con il tempo non hanno più trovato giustificazione. Il *web*, infatti, se, da un lato, ha offerto e offre soluzioni nuove per le operazioni finanziarie, dall'altro, ha fornito la possibilità alla criminalità di giovarsi di innovativi metodi di riciclaggio o di finanziamento al terrorismo.[9]

Tuttavia, il legislatore europeo si è ben presto reso conto dei rischi connessi ai prestatori di servizi di cambio tra valute virtuali e valute legali. Le prime, infatti, beneficiando di un maggior grado di anonimato rispetto ai classici trasferimenti di fondi, possono essere utilizzate per nascondere trasferimenti finanziari, anche importanti, nell'assenza di qualunque tipo di monitoraggio da parte delle Autorità pubbliche e di norme vincolanti sulle condizioni di questo monitoraggio, sia a livello sovranazionale, che dei singoli Stati membri. Possibilità che di fatto si è verificata.

Da qui la necessità di un nuovo intervento legislativo europeo e di una nuova Direttiva, da un lato, per contrastare più efficacemente il finanziamento del terrorismo e il riciclaggio, avuto, appunto, riguardo dei nuovi strumenti di pagamento nei mercati finanziari come le valute virtuali, e, dall'altro, per stimolare l'adozione di ulteriori misure volte a garantire la maggiore trasparenza delle operazioni finanziarie, delle società e degli altri soggetti giuridici, come i *trust*, per migliorare l'attuale quadro di prevenzione.

Come si avrà modo di precisare meglio in seguito, la nuova Direttiva, proseguendo la strada tracciata dalla precedente, si prefigge l'obiettivo di trovare un equilibrio fra gli interessi in gioco rappresentati, per un verso, dalla protezione della società dalla criminalità e, per altro verso, dalla salvaguardia della stabilità e dell'integrità del sistema finanziario dell'Unione Europea.

2.2. *La Direttiva n. 843/2018/UE e le differenze con la normativa nazionale prevista dal D.lgs. n. 90/2017.*

Da quanto esposto in precedenza emerge come siano state molteplici le ragioni che hanno condotto ad intervenire sulla IV Direttiva antiriciclaggio e ad approvare la Direttiva n. 843/2018/UE per contrastare in modo più incisivo il riciclaggio e il finanziamento del terrorismo.

Con riguardo più specificamente ai passaggi che storicamente hanno portato all'approvazione della V Direttiva, è bene chiarire che, a fine 2015, dopo i tragici fatti di terrorismo che avevano interessato i Paesi del nord Europa, il Consiglio dell'Unione Europea e il Consiglio Europeo avevano richiesto un rafforzamento della normativa di contrasto in materia. Nel luglio del 2016, la Commissione Europea aveva proceduto a pubblicare la Proposta (COM 2016/450) di modifica della IV Direttiva, già in corso di recepimento da parte dei Paesi europei. Proposta che, per ciò che qui interessa, prevedeva l'aspetto della lotta al riciclaggio e ai rischi di finanziamento del terrorismo attraverso il sistema delle valute virtuali. La Commissione proponeva, in particolare, di includere, nell'ambito di applicazione della Direttiva antiriciclaggio, le piattaforme di scambio di valute virtuali e i prestatori di servizi di portafoglio digitale, con la conseguenza che anche tali soggetti sarebbero stati chiamati ad applicare gli obblighi di adeguata verifica della clientela alle operazioni di cambio di valute virtuali in valute reali, ponendo fine all'anonimato associato a detti scambi, ragione principale della loro fortuna

[9] Salvini (2015), p. 203.

quale strumento per porre in essere indisturbatamente attività criminose. Tali previsioni sono poi confluite nella V Direttiva antiriciclaggio (n. 843/2018/UE).

Già la Banca Centrale Europea, in sede di parere della Proposta di modifica della IV Direttiva, aveva mostrato le proprie preoccupazioni in relazione alle valute virtuali e alle differenze tra le stesse e le c.d. valute legali, quali la volatilità associata alle prime, comunemente più elevata di quella delle valute emesse da banche centrali o la cui emissione sia da queste comunque stata autorizzata; volatilità, inoltre, non sempre correlata a fattori economici o finanziari. Altri motivi di preoccupazione mostrati dalla BCE erano stati la circostanza che, a differenza dei possessori di monete legalmente istituite, i detentori di monete virtuali non hanno la garanzia di poterle cambiare in futuro con beni e servizi o con moneta legalmente istituita; nonché l'affidamento riposto dagli operatori economici sulle valute virtuali, che, in caso di notevole futuro incremento, può potenzialmente incidere sul controllo esercitato dalle banche centrali sull'offerta di moneta, con rischi per la stabilità dei prezzi.[10]

Ad un'analisi più ravvicinata della V Direttiva si nota la fondamentale circostanza che, mentre le precedenti Direttive europee in materia di antiriciclaggio hanno generalmente fatto seguito alle Raccomandazioni pubblicate dal GAFI in ambito OCSE[11], la V Direttiva antiriciclaggio, invece, non è stata preceduta da una nuova versione delle Raccomandazioni del GAFI. L'aggiornamento del 2016 delle Raccomandazioni GAFI del 2012, infatti, non indica i profili specifici contenuti della V Direttiva, che, come accennato, è volta essenzialmente ad adeguare la normativa di settore ai rischi connessi alle valute virtuali. Ciò in quanto le Raccomandazioni internazionali in materia di criptovalute e rischi di riciclaggio erano già state formulate al momento dell'adozione della Direttiva del 2015.[12]

Ciò premesso, la Direttiva del 2018, con riguardo alle *virtual curriencies,* interviene ampliando soggettivamente la portata della normativa antiriciclaggio, includendovi, come accennato, anche i prestatori di servizi di cambio tra valute virtuali e valute legali e i prestatori di servizi di portafoglio digitale.

In relazione a ciò, in verità, l'Italia disponeva già prima dell'adozione della menzionata Direttiva di una legislazione innovativa e anticipatrice, spinta dalla particolare sensibilità del sistema economico italiano ai fenomeni di criminalità.

In particolare, il D.lgs. n. 90/2017, nell'attuare la Direttiva del 2015, precorrendo l'orientamento del legislatore europeo, aveva provveduto a fornire una definizione di "valuta virtuale"[13]

[10] Così si legge nel Parere della Banca Centrale Europea del 12 ottobre 2016.

[11] Più specificamente, la I Direttiva, n. 308/1991/CE, fissava gli obblighi di identificazione, registrazione e segnalazione di operazioni sospette, ponendoli a carico dei soli enti creditizi e finanziari. Ad essa l'Italia si è adeguata con il d.l. n. 143/1991, recante "*Provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio*". Dieci anni dopo, la II Direttiva, n. 97/2001/CE, estendeva l'ambito di applicazione degli obblighi suddetti anche ai professionisti; tale Direttiva in Italia è stata ratificata attraverso il D.Lgs. n. 56/2004, in vigore fino al 29 dicembre 2007, in quanto abrogato dall'art. 64, lett. d) del D.Lgs. n. 231/2007. La III Direttiva, n. 60/2005/CE, invece, applicava al contrasto del terrorismo internazionale le metodologie e gli obblighi già sperimentati contro il riciclaggio del denaro sporco; con essa vengono abrogate le precedenti Direttive e recepite le 40 Raccomandazioni della FAFT. Alla Direttiva è stata data attuazione in Italia attraverso il D.Lgs. n. 231/2007. Infine, la IV Direttiva, n. 849/2015/UE, facendo seguito alle nuove Raccomandazioni GAFI del 2012, recava importanti novità di sistema quali l'obbligo di criminalizzare i reati fiscali, facendone così presupposto del riciclaggio, l'istituzione di un registro nazionale dei beneficiari effettivi e l'assoggettamento a stringenti controlli per l'operatività delle persone politicamente esposte.

[12] Il report del GAFI, "*Virtual Currencies – Potential AML/CFT Risks*", del giugno 2014 auspicava un intervento delle istituzioni europee per definire un quadro normativo armonizzato che riservasse l'operatività in valute virtuali a soggetti autorizzati, per i rischi di ricostruzione della traccia finanziaria posti dal loro anonimato, dalla mancanza di norme e di autorità di controllo, dalla complessità delle strutture usate e dei soggetti coinvolti, distribuiti tra diversi Paesi e giurisdizioni. Nello stesso senso, nel luglio 2014, la *European Banking Authority,* nel suo "*Opinion on 'virtual currencies*", individuava i profili di rischio che la negoziazione delle criptovalute poteva comportare per gli utilizzatori, i partecipanti al mercato, l'integrità e la stabilità del sistema finanziario e del sistema dei pagamenti, gli intermediari e le autorità di regolamentazione. Il documento si chiudeva auspicando anch'esso un intervento delle istituzioni europee per definire un quadro normativo armonizzato, che riservasse l'operatività in valute virtuali a soggetti autorizzati. Nel gennaio 2015, infine, anche l'Unità di Informazione Finanziaria italiana, nel documento "*Utilizzo anomalo delle valute virtuali*", sottolineava i potenziali effetti per il riciclaggio ed il finanziamento del terrorismo resi possibili dall'anonimato delle transazioni in valute virtuali, dall'operatività *on line* e dal fatto che le operazioni effettuate con valute virtuali avvengono fra soggetti che possono operare in Stati diversi, anche in Paesi a rischio.

[13] La nozione di moneta virtuale fornita dal D.Lgs. n. 90/2017 è sovrapponibile a quella prevista già dalla Proposta di modifica avanzata dalla Commissione poi confluita nella V Direttiva. In particolare, ai sensi dell'art. 1, co. 2, lett. qq), D.Lgs. n. 231/2007 come modificato dal D.Lgs. n. 90/2017 per moneta virtuale si intende la "*rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente*". Rispetto alle definizioni sinora elaborate è posto in risalto l'impiego delle valute virtuali quale mezzo di scambio, restando invece tralasciata la loro possibile detenzione a scopo di investimento.
Prima di allora l'ordinamento nazionale era sprovvisto di una definizione delle valute virtuali, tematica affidata agli esercizi della dottrina e delle autorità pubbliche, sovente carenti di visione organica, nella consapevolezza del carattere relativo di ogni catalogazione. In dottrina si ricorda Bocchini (2017), p. 27.
La Direttiva 2018, aggiungendo il punto 18) alla Direttiva del 2015, prevede quanto segue:

e, poi, ad inserire tra i soggetti tenuti al rispetto delle regole antiriciclaggio "*i prestatori di servizi relativi all'utilizzo di valuta virtuale, limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso* (*c.d.* exchange)".

Tuttavia, sul punto occorre fare una precisazione.

In Italia l'estensione della disciplina antiriciclaggio operata dal citato D.lgs. del 2017 ha riguardato i soli *exchangers* (o *virtual currency exchangers*), cioè coloro (persone fisiche o giuridiche) che offrono agli *users* servizi di cambio di moneta virtuale con moneta legale o metalli preziosi (e viceversa), in cambio di una commissione.[14] Tale estensione era stata dettata dalla constatazione che tali soggetti sono gli unici operatori che, occupandosi del cambio fra criptovalute e moneta reale, sono in grado di identificare le persone che danno luogo a tali transazioni. Nella prospettiva legislativa, pertanto, la regolamentazione degli *exchangers* avrebbe dovuto condurre al massimo effetto con il minimo investimento di risorse e massima concentrazione dei controlli.[15]

Come accennato, il D. Lgs. n. 90/2017[16] ha introdotto per gli "scambiatori" l'obbligo di iscrizione in una sezione speciale del registro dei cambiavalute tenuto dall'Organismo degli Agenti e dei Mediatori, *ex* art. 128 *undecies* TUB, parificandoli così ai tradizionali cambiavalute e sottoponendoli, pertanto, alle disposizioni antiriciclaggio.[17] In virtù di queste disposizioni essi sono tenuti all'adempimento degli obblighi di adeguata verifica della clientela, di cui agli artt. 17 ss. del D.lgs. n. 231/2007, nonché alla conservazione dei documenti, dei dati e delle informazioni raccolte (*ex* artt. 31 e ss.). Inoltre, qualora nutrano il sospetto che l'attività di cambio sia riconducibile ad operazioni di riciclaggio, sono tenuti a segnalare l'operazione sospetta alla Unità di Informazione Finanziaria italiana.

In tema di adeguata verifica della clientela, in particolare, l'art. 18 del D.lgs. n. 231/2007 impone una nutrita serie di adempimenti formali: l'identificazione e la verifica dell'identità del cliente o dell'esecutore attraverso un documento d'identità, nonché sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile; l'identificazione e la verifica dell'identità del titolare effettivo attraverso l'adozione di misure proporzionate al rischio ivi comprese, con riferimento alla titolarità effettiva di persone giuridiche, le misure che consentano di ricostruire l'assetto proprietario e di controllo del cliente; l'acquisizione e la valutazione di informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale; il controllo costante del rapporto con il cliente, per tutta la sua durata, la verifica e l'aggiornamento dei dati e delle informazioni acquisite nello svolgimento delle attività summenzionate, anche riguardo al controllo della provenienza dei fondi e delle risorse nella disponibilità del cliente.

Se questi sono gli obblighi di adeguata verifica della clientela a cui sono tenuti i soggetti obbligati è evidente che l'anonimato che caratterizza il sistema delle valute virtuali non agevola il loro assolvimento, specie con riferimento all'identificazione del titolare effettivo.[18]

Nel caso di inosservanza dei suddetti obblighi relativi agli *exchangers* possono essere contestate una o più delle fattispecie penali delineate dall'art. 55 del D.lgs. n. 231/2007 citato, che punisce le violazioni gravi degli obblighi previsti legislativamente caratterizzate da fraudolenza. Il riferimento è, nella specie, all'inosservanza degli obblighi di adeguata verifica della clientela mediante falsificazione dei dati e delle informazioni relative al cliente o l'utilizzo di

"18) «*valute virtuali*»: *una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente*".

Il successivo punto 19), invece, definisce il «*prestatore di servizi di portafoglio digitale*». Tale è "*un soggetto che fornisce servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*".

[14] Quali strumenti di pagamento gli *exchangers* ammettono, oltre che il denaro contante, i bonifici bancari, le carte di credito e le valute virtuali.

[15] Majorana (2018), p. 634.

[16] Attraverso una modifica della normativa prevista dall'art. 17 *bis* del D. Lgs. n. 141 del 13 agosto 2010, a cui sono stati aggiunti i commi 8 *bis* e 8 *ter*.

In particolare, l'art. 17 *bis,* co. 8 *bis,* prevede che: "*Le previsioni di cui al presente articolo si applicano, altresì, ai prestatori di servizi relativi all'utilizzo di valuta virtuale, come definiti nell'art. 1, co. 2, lett. ff), del D.lgs. 21 novembre 2007, n. 231, e successive modificazioni tenuti, in forza della presente disposizione, all'iscrizione in una sezione speciale del registro di cui al co. 1*".

Il successivo comma 8 *ter*, invece, dispone che: "*Ai fini dell'efficiente popolamento della sezione speciale di cui al comma 8* bis, *con decreto del Ministro dell'economia e delle finanze sono stabilite le modalità e la tempistica con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale sono tenuti a comunicare al Ministero dell'economia e delle finanze la propria operatività sul territorio nazionale. La comunicazione costituisce condizione essenziale per l'esercizio legale dell'attività da parte dei suddetti prestatori. Con il decreto di cui al presente comma sono stabilite forme di cooperazione tra il Ministero dell'economia e delle finanze e le forze di polizia, idonee ad interdire l'erogazione dei servizi relativi all'utilizzo di valuta virtuale da parte dei prestatori che non ottemperino all'obbligo di comunicazione*".

[17] Accinni (2018), p. 20.

[18] Majorana (2018), p. 635.

tali dati; alla violazione degli obblighi di conservazione mediante l'acquisizione di dati falsi, informazioni non veritiere o tramite il ricorso a mezzi fraudolenti per pregiudicare la corretta conservazione dei dati; alla violazione dell'obbligo di fornire dati e informazioni per l'adeguata verifica con omissione o consegna di dati falsi e, infine, alla comunicazione a terzi dell'avvenuta segnalazione. 19

Inoltre, agli *exchangers* che non dovessero segnalare operazioni sospette si potrebbe astrattamente contestare un concorso nell'altrui reato di riciclaggio, di cui all'art. 648 *bis* c.p., dovendo in ogni caso essere provata la sussistenza dell'elemento psicologico del reato, ossia il dolo generico, consistente nella rappresentazione della provenienza delittuosa dei beni e nella volontà di compiere le attività relative ad impedire l'identificazione della provenienza delittuosa stessa, ciò in conformità con quanto stabilito dalla Corte di Cassazione nell'ipotesi di un direttore di banca che aveva autorizzato operazioni sospette.[20]

A quanto fino a qui detto si aggiunga, infine, che esistono diverse tipologie di *exchangers*. Vi sono quelli che impongono il contatto fisico con il cliente e quelli virtuali. Mentre i primi possono seguire le normali procedure di adempimento per la verifica della clientela, i secondi restano nel limbo, considerato che la previsione di identificazione a distanza necessita di idonee forme e modalità (art. 19, co. 1, n. 5, D.Lgs. n. 231/2007) che, però, non sono ancora state definite dalle autorità di settore.[21] È, pertanto, evidente che alla diversa natura degli *exchangers* corrispondono problematiche diverse.[22]

Nonostante le ragionevoli motivazioni che hanno condotto all'estensione della normativa antiriciclaggio ai soli *exchangers*, di cui si è detto, tale previsione era stata oggetto di critica, ancora una volta, da parte della Banca Centrale Europea, perché giudicata insufficiente. Ciò in quanto il ruolo svolto dagli "scambiatori" nel palcoscenico del sistema di criptovalute è meramente eventuale, perché, da un lato, qualunque privato che intende procurarsi moneta virtuale non deve necessariamente rivolgersi ad una società professionista di *exchange* per ottenere la valuta in questione, dall'altro, la valuta virtuale profitto del reato presupposto non deve obbligatoriamente essere scambiata in moneta reale, potendo continuare a circolare nel mondo virtuale o essere scambiata con ulteriori valute convertibili, che potrebbero trovare la via d'uscita senza passare dai soggetti obbligati.[23]

Anche per ovviare all'insufficienza già emersa con riguardo alla normativa italiana la Direttiva del 2018 ha esteso l'applicazione della disciplina antiriciclaggio anche ai c.d. *wallet providers*, cioè coloro che rendono un servizio di conservazione (*storage*) di criptovalute a favore degli utenti delle stesse dietro corrispettivo.[24] Essi facilitano l'esecuzione delle transazioni non solo con gli *exchangers*, ma anche con i *merchants,* che accettano di ricevere valuta virtuale in cambio della fornitura di beni o servizi. Anche i *wallet providers*, quindi, svolgono un'attività "ponte" tra il mondo reale delle valute aventi corso legale e quello virtuale delle criptovalute.[25] Tuttavia, a ben vedere, anche il ruolo di questi ultimi si rivela eventuale, essendo discrezionale la scelta di depositare le proprie criptovalute in un portafoglio elettronico, c.d. *wallet,* potendo l'utente, invece, conservare le proprie monete nel "portfolio" personale.[26] Anche rispetto a questa estensione, peraltro, la Banca Centrale Europea si era mostrata critica.

Da quanto fin qui esposto emerge che la scelta di sottoporre alla disciplina antiriciclaggio soggetti solo eventualmente ricompresi nella transazione non è utile ad affievolire l'elevata minaccia di riciclaggio intrinsecamente presente nelle caratteristiche delle monete virtuali. A ciò

[19] Lucev e Boncompagni (2018), pp. 3-4.
[20] Cass. pen., Sez. II, 14 gennaio 2016, n. 9472.
[21] Art. 19, comma 1, n. 5):
"*1. I soggetti obbligati assolvono agli obblighi di adeguata verifica della clientela secondo le seguenti modalità:*
a) l'identificazione del cliente e del titolare effettivo è svolta in presenza del medesimo cliente ovvero dell'esecutore, anche attraverso dipendenti o collaboratori del soggetto obbligato e consiste nell'acquisizione dei dati identificativi forniti dal cliente, previa esibizione di un documento d'identità in corso di validità o altro documento di riconoscimento equipollente ai sensi della normativa vigente, del quale viene acquisita copia in formato cartaceo o elettronico. Il cliente fornisce altresì, sotto la propria responsabilità, le informazioni necessarie a consentire l'identificazione del titolare effettivo. L'obbligo di identificazione si considera assolto, anche senza la presenza fisica del cliente, nei seguenti casi:
(…)
5) per i clienti i cui dati identificativi siano acquisiti attraverso idonee forme e modalità, individuate dalle Autorità di vigilanza di settore, nell'esercizio delle attribuzioni di cui all'articolo 7, comma 1, lettera a), tenendo conto dell'evoluzione delle tecniche di identificazione a distanza…".
[22] Majorana (2018), p. 630.
[23] In tal senso il citato Parere della Banca Centrale Europea del 12 ottobre 2016.
[24] Tale servizio è assimilabile a quello previsto dall'art. 1834 c.c., rubricato "*Depositi di danaro*".
[25] La Rocca (2015), p. 210.
[26] Messina (2017), p. 381.

si aggiunga che nella vigenza della vecchia Direttiva solo il nostro Paese aveva previsto l'estensione agli *exchangers* degli obblighi derivanti dalla normativa antiriciclaggio; tale circostanza evidentemente riduceva drasticamente l'efficacia delle nuove disposizioni, stante la facilità di operare *on line* su altre aree geografiche non altrettanto avanzate dal punto di vista normativo, e la conseguente possibilità di una facile elusione della normativa italiana.

Ciò nonostante, non può tacersi che diversi Stati dell'Unione Europea già nel vigore della Direttiva del 2015, avevano avvertito la necessità di intervenire in materia, attraverso proposte di regolamentazione adeguata delle valute virtuali, per contrastare il loro uso illecito e sottoporle ad adeguati controlli, a tutela degli investitori e del sistema finanziario tutto.

In Germania, ad esempio, le criptovalute sono oramai pacificamente ritenute unità di conto e, dunque, strumenti finanziari ai sensi della normativa nazionale, e come tali vengono regolamentate. In Francia, invece, una commissione del Ministero delle Finanze è impegnata nella redazione di regole per vigilare sullo sviluppo delle valute virtuali con lo scopo di evitare rischi di speculazione e manipolazione finanziaria.[27]

La nuova Direttiva, prevedendo l'estensione a livello sovranazionale della normativa antiriciclaggio ai prestatori di servizi di cambio tra valute virtuali e legali e ai prestatori di servizi di portafoglio digitale, dovrebbe condurre ad un superamento di tale situazione frammentaria ed a una regolamentazione più unitaria del settore.[28] È chiaro, infatti, che la condizione necessaria per un adeguato sistema di contrasto al riciclaggio e al finanziamento del terrorismo è l'armonizzazione della risposta punitiva, attuata mediante un sistema di sanzioni e misure comuni, da adottarsi almeno con riguardo alle violazioni gravi, ripetute o sistematiche degli obblighi relativi alle misure di adeguata verifica della clientela, alla conservazione dei documenti, alla segnalazione delle operazioni sospette e controlli interni dei soggetti obbligati.[29]

Infine, l'ultima novità interessante della Direttiva n. 843/2018/UE è rappresentata dalla possibilità per le *Financial Intelligence Unit* di ciascun Paese membro di ottenere le informazioni che consentano di associare gli indirizzi della valuta virtuale alla reale identità del proprietario della stessa e l'ulteriore possibilità di "*consentire agli utenti di presentare, su base volontaria, un'autodichiarazione alle autorità designate*".[30] Queste previsioni mirano precipuamente ad erodere, per quanto possibile, il carattere dell'anonimato delle criptovalute, per ottenere una maggiore trasparenza del sistema e, per tale via, una maggiore possibilità di controllo pubblico dello stesso. L'applicazione pratica di questa ultima previsione può riservare interessanti sviluppi nel contrasto al riciclaggio commesso attraverso le valute virtuali.

3. Osservazioni conclusive: quali prospettive per il futuro?

Alla luce di quanto esposto fino a qui è possibile svolgere qualche riflessione.

L'innovativo meccanismo delle valute virtuali ha enormi potenzialità e rappresenta una opportunità di sviluppo importante del sistema finanziario. La criptovaluta, come chiarito, infatti, cumula in sé i vantaggi della moneta elettronica e del contante; il sistema consente la consegna digitale *brevi manu* di valute virtuali in pochi minuti, in qualsiasi parte del mondo. Il "tempo" diviene un fattore neutrale, che non arreca vantaggi o danni ad alcuna delle controparti, con la conseguenza che le criptovalute non sono legate a fenomeni quali l'inflazione, gli interessi e il costo associato alla proprietà o al possesso di valuta reale.[31] L'utilizzo del *web,* poi, come luogo di negoziazione rende il sistema accessibile ad una enorme platea di potenziali investitori, favorendone l'ascesa e il carattere transfrontaliero. A ciò si aggiunga, infine, che le valute virtuali rappresentano il traguardo dei sostenitori di quella corrente di pensiero, promotrice di una democratizzazione del sistema finanziario, caratterizzata dall'assenza di intermediari e di controllo statale, diretta alla creazione di una economia e di un mercato liberi, contraddistinti da una regolamentazione rimessa in via esclusiva alla *community* degli utenti.[32]

Sarebbe, tuttavia, ingenuo pensare alle valute virtuali come esenti da criticità.

[27] Di Vizio (2018), p. 25.
[28] A riprova di ciò, qualche settimana fa l'Irlanda ha adottato un progetto di legge di attuazione della V Direttiva europea finalizzato ad estendere ai prestatori di valute virtuali e ai *wallet providers* la disciplina antiriciclaggio.
[29] Salvini (2016), p. 166.
[30] Così l'art. 65, rubricato "*Relazione*", della Direttiva del 2015 come sostituito dalla Direttiva del 2018.
[31] Chiriatti (2015).
[32] Sturzo (2018), p. 20.

In particolare, la volatilità dei prezzi che le caratterizza, potenzialmente sfruttabile dai soggetti con maggiori competenze tecnologiche; il loro consistente sviluppo fuori dei confini della regolamentazione finanziaria, più incline ai fenomeni fraudolenti; l'utilizzo di piattaforme di scambio prive di disciplina e di protezioni legali per le perdite connesse ai fondi detenuti sui portafogli digitali presenti su di esse, con il rischio di una perdita definitiva del capitale investito nel caso di un loro fallimento; nonché la non impermeabilità dei portafogli digitali agli *hackers* sono aspetti che preoccupano e che impongono di verificare in che termini il diritto penale può oggi fronteggiare i profili più pericolosi del fenomeno e soddisfare le esigenze di protezione che essi impongono.[33]

In generale, l'assenza di una cornice legislativa chiara e la situazione di totale incertezza giuridica in cui le valute virtuali sono state utilizzate fin dalla loro nascita hanno costituito fattori di agevolazione della possibilità di un uso distorto delle stesse per la realizzazione di attività criminali. E a fronte di un utilizzo illecito delle criptovalute sempre più diffuso, una effettiva attività di contrasto a tale tendenza richiede un adeguamento degli strumenti di prevenzione e di contrasto, non tanto sul piano della tipizzazione di nuove fattispecie penali, ritenendosi quelle esistenti adeguate, quanto, piuttosto, su quello della disciplina preventiva, rispetto alla quale servono regole più efficaci. Se è vero, infatti, che l'attività di prevenzione consente di intercettare anticipatamente le infiltrazioni criminali nel sistema legale, attraverso il potenziamento di strumenti preventivi si può agire per impedire che, come già avvenuto, le valute virtuali, vengano utilizzate per facilitare la realizzazione di reati gravi e di forte allarme sociale come quelli legati al terrorismo o distorsivi dell'economia legale come, per quello che qui interessa, il riciclaggio.

Di certo, l'aver provveduto ad estendere, prima a livello nazionale e poi a livello europeo, la platea dei soggetti sottoposti alla normativa antiriciclaggio ha rappresentato un passo importante, sul piano preventivo, per il contrasto al riciclaggio realizzato attraverso valute virtuali, in quanto tale estensione è funzionale a garantire una risposta al fenomeno più forte e unitaria a livello sovranazionale, con importanti riflessi anche sul piano dei singoli Stati membri. Come già accennato, infatti, un meccanismo di contrasto efficace al sistema criminale predetto passa necessariamente dall'armonizzazione della risposta punitiva.

Tuttavia, ciò potrebbe non essere decisivo, in quanto la necessità di sottoporre alla disciplina antiriciclaggio i soggetti che operano con le valute virtuali finisce inevitabilmente per cozzare con le caratteristiche proprie delle stesse, l'anonimato e la scarsa tracciabilità *in primis*, e ciò rende gli effetti di tale estensione parziali e non sempre soddisfacenti in un'ottica di contrasto preventivo.

A riprova di ciò, l'impossibilità tecnica di seguire il denaro (*follow the money*) sul *web*, come avviene normalmente al fine di accertare e contestare reati come il riciclaggio, ha portato a poterlo registrare e monitorare solamente in uscita dal mondo reale o attenderlo al momento dell'uscita dal mondo virtuale (*wait for the money*).[34] Da qui l'estensione in termini di applicabilità della normativa antiriciclaggio a coloro che in queste fasi operano; il riferimento è, in primo luogo, agli "scambiatori" di moneta virtuale in moneta legale, come è avvenuto in Italia. Come già visto, però, l'estensione soggettiva della normativa antiriciclaggio non è stata priva di critiche, in quanto essa ha interessato soggetti non necessariamente ricompresi nella transazione, con la conseguenza che tale ampliamento non ha smorzato significativamente la minaccia di riciclaggio presente nelle caratteristiche proprie delle criptovalute. Senza trascurare i problemi connessi all'assenza di regolamentazione di settore per alcuni di questi soggetti, come gli *exchangers* c.d. virtuali, che restano nel limbo circa le modalità di controllo della clientela a distanza, che necessita di forme e modalità idonee non ancora definite dalle autorità di settore.

D'altro canto, però, come è stato condivisibilmente osservato, «*fino a quando non sarà possibile istituire regole che presiedano la rete dall'interno, sarà necessario costruire una "cinta daziaria" dotata di alcune "porte" per individuare chi e che cosa passa dal mondo reale a quello virtuale e viceversa*».[35] Quanto detto fino a qui dimostra che quello dei soggetti cui applicare la disciplina antiriciclaggio continua ad essere un aspetto importante su cui riflettere, soprattutto in vista dell'applicazione della nuova Direttiva.

Sul punto, peraltro, la stessa V Direttiva antiriciclaggio non ha mancato di richiamare

[33] Di Vizio (2018), p. 23.
[34] Majorana (2018), p. 634.
[35] Majorana (2018), p. 630.

le autorità competenti a potenziare la propria capacità di monitorare, attraverso i soggetti obbligati, l'uso delle valute virtuali, in modo da consentire un approccio equilibrato e proporzionale, a tutela dei progressi tecnici e dell'elevato livello di trasparenza raggiunto in materia di finanziamenti alternativi.[36]

In ultima analisi, consapevoli delle criticità e delle opportunità proprie delle nuove tecnologie quali le criptovalute, l'obiettivo da perseguire per il futuro deve essere quello di garantire l'eventuale sviluppo di nuovi mercati finanziari in modo compatibile con la tutela del sistema economico-finanziario e dei soggetti che a vario titolo vi operano[37], rafforzando le attività e gli strumenti di prevenzione e di monitoraggio degli stessi, tanto a livello nazionale, che sovranazionale, anche attraverso il ricorso ad agenzie di supporto private, quali *Elliptic* e *Chainalysis*, le quali dispongono di conoscenze specifiche e *software* dedicati al riconoscimento degli schemi di riciclaggio che spesso mancano alle Autorità pubbliche.

Bibliografia

Accinni, Giovanni Paolo (2018): "Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017)", *www.archiviopenale.it*, 1, pp. 1- 20

Amato, Massimo e Fantacci, Luca (2016): "Per un pugno di *Bitcoin* – Rischi e opportunità delle monete virtuali", (Milano, Università Bocconi Editore)

Bocchini, Roberto (2017): "Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche", *Diritto dell'Informazione e dell'Informatica*, 1, pp. 27 -52

Capaccioli, Stefano (2015): "Criptovalute e *bitcoin*: un'analisi giuridica", (Milano, Giuffrè)

Chiriatti, Massimo (2015): "Con i *bitcoin* il tempo non è più denaro", *http://www.economopoly.ilsole24ore.com/2015/08/01/con-i-bitcoin-il-tempo-non-epiudenaro/*

D'Agostino, Luca (2017): "Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D. Lgs. 90/2017", *Rivista di Diritto Bancario*, *http://www.dirittobancario.it/rivista//fianza/mercati-finanziari-e-regole-di-sistema/operazioni-emissione-cambio-e-trasferimento-criptovaluta-considerazioni*

De Flammineis, Siro (2017): "Gli strumenti di prevenzione del riciclaggio - L'esperienza italiana nel quadro della quarta direttiva europea e prime osservazioni sullo schema di decreto attuativo", *Diritto penale contemporaneo – Rivista trimestrale*, 5, pp. 259 -270

Di Vizio, Fabio (2018): "Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti. Lo statuto delle valute virtuali: le discipline e i controlli", *Diritto penale contemporaneo – Rivista trimestrale*, 10, pp. 21-81

Giacometti, Tatiana e Formenti, Oliviero (2017), "La nuova disciplina del riciclaggio e di finanziamento del terrorismo", *Diritto penale contemporaneo – Rivista trimestrale*, 7-8, pp. 195-198

La Rocca, Laura (2015): "La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali", *Analisi Giuridica dell'Economia,* 1, pp. 201-222

Lucev, Riccardo e Boncompagni, Federico (2018): "Criptovalute e profili di rischio penale nella attività degli *exchanger*", *Giurisprudenza penale web*, 3, pp. 1-8

[36] Di Vizio (2018), p. 81.
[37] La Rocca (2015), p. 222.

Majorana, Daniele (2018): "Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal *web*", *Corriere tributario*, 8, pp. 630-636

Messina, Enrico (2017): "*Bitcoin* e riciclaggio", in Quattrociocchi, Bernardino (a cura di): *Norme, regole e prassi nell'economia dell'antiriciclaggio internazionale* (Torino, Giappichelli), pp. 381-386

Romano, Francesca (2018): "Disciplina in materia di prevenzione del riciclaggio e del terrorismo", in Antolisei, Francesco: *Manuale di diritto penale, Leggi complementari*, vol. I, XV, Grosso, Carlo Federico (a cura di), (Milano, Giuffrè), pp. 597-613

Rossi, Alessandra (2018): "Prevenzione del riciclaggio e finanziamento del terrorismo: finalità e novità normative", *Diritto penale e processo*, 1, pp. 25-41

Salvini, Omar (2015): "Potenziamento e proroga dell'impiego del personale militare appartenente alle Forze armate", in AA.VV.: *Antiterrorismo. Commento organico al d.l. 18 febbraio 2015* (Roma, Dike), pp. 203-220

Salvini, Omar (2016): "Il contrasto all'abuso del sistema finanziario per scopi di riciclaggio e finanziamento del terrorismo: la IV Direttiva (EU) 2015/849, tra coordinamento e cooperazione", *Rivista italiana di diritto pubblico comunitario*, pp. 148-188

Sorbello, Pietro (2015): "Segnalazione di operazioni sospette e posizione di garanzia. ammissibilità e limiti del concorso per omissione nel delitto di riciclaggio", *L'Indice Penale*, pp. 437- 471

Sturzo, Ludovica (2018): "*Bitcoin* e riciclaggio 2.0", *Diritto penale contemporaneo – Rivista trimestrale,* 5, pp. 19-34

Troyer, Luca e Zancan, Monica (2017): "Verso una nuova Direttiva in materia di prevenzione del riciclaggio e di finanziamento del terrorismo", *Diritto penale contemporaneo – Rivista trimestrale*, 3, pp. 365-369

Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione

Las monedas virtuales y los ontológicos riesgos de lavado de activos: técnicas de represión.

Virtual currencies and the endemic risk of money laundering: repression techniques

Fabiana Pomes
Dottoranda in Diritto e Impresa presso l'Università Luiss G. Carli
fpomes@luiss.it

Riciclaggio | Lavado de activos | Money Laundering

Abstracts

Il fenomeno delle valute virtuali, di cui il *Bitcoin* costituisce l'esempio più noto, ha assunto nell'ultimo decennio connotati di sempre maggiore rilevanza e centralità in ambito nazionale e sovranazionale. Il presente contributo si pone l'obiettivo di analizzare il rischio di un utilizzo anomalo della valuta virtuale e la possibilità che tale strumento di pagamento *on-line* venga "piegato" ad attività criminali. L'attenzione si soffermerà sulle connotazioni peculiari della valuta virtuale, evidenziando come le stesse la rendano idonea, per sua natura, a "dissimulare" il valore oggetto del suo trasferimento nella sconfinata realtà virtuale e, quindi, a porsi come volano per la commissione dei reati di riciclaggio e autoriciclaggio. Ci si soffermerà sul fronte repressivo e sulla possibilità di ricondurre i fenomeni *cyber-laundering* e *self-cyberlaundering* nell'alveo delle fattispecie codicistiche previste dagli artt. 648-*bis* e 648-*ter*1 c.p., senza che ciò determini una indebita e vietata applicazione analogica.

El fenómeno de las monedas virtuales, del cual el Bitcoin constituye el ejemplo más conocido, ha asumido en el último decenio connotaciones de siempre mayor relevancia en el ámbito nacional e internacional. El presente trabajo tiene por objeto analizar el riesgo de un uso anómalo de las monedas virtuales y de la posibilidad de que ellas sean utilizadas en actividades criminales. Se prestará particular atención a las características propias de la moneda virtual, evidenciando cómo las mismas la convierten en un instrumento idóneo para disimular el valor objeto de su transferencia en la realidad virtual, convirtiéndose de esta manera en una posible herramienta para la comisión de delitos de lavado de activos. Finalmente, se aborda la discusión sobre si las conductas de ciber-lavado de activos pueden ser sancionadas en virtud de los artículos 648-bis y 648ter1 del código penal italiano, sin que ello signifique una indebida y prohibida aplicación analógica.

The phenomenon of virtual currencies, among which the Bitcoin is a renowned example, has become increasingly relevant in this decade both at a national and a supranational level. This paper aims to analyze the risk of unlawful use of virtual currency and the possibility that such an instrument for on-line transactions is used for criminal activities. The focus will be on the peculiarities of virtual currencies, highlighting how they can be apt to "conceal" the value transferred in the borderless virtual world, so being potentially instrumental to money laundering and self-money laundering. Then the repression will be analyzed, also in order to assess if cyber-laundering and self-cyberlaundering can be subsumed in the criminal provisions under articles 648-*bis* and 648-*ter*1 of the Italian Criminal Code without any breach of the nullum crimen sine lege principle as a consequence of analogy.

Sommario

1. Rilievi introduttivi.

Quello delle c.d. valute virtuali, di cui il *Bitcoin* costituisce l'esempio più noto, è un fenomeno che si diffonde nella prassi con crescita esponenziale e che, essendo privo di una compiuta disciplina giuridica, pone delle esigenze di regolamentazione tanto a livello nazionale quanto a livello sovranazionale.

Il presente contributo si pone l'obiettivo di analizzare il rischio di un utilizzo anomalo della valuta virtuale e la possibilità che tale strumento di pagamento *on-line* venga "piegato" ad attività criminali; in particolare, la criptovaluta sembra idonea, per sua natura, a "dissimulare" il valore oggetto del suo trasferimento nella sconfinata realtà virtuale[1] e, quindi, a porsi come volano per la commissione dei reati di riciclaggio e autoriciclaggio, nonché come ostacolo alla prevenzione degli stessi.

Di recente, si è assistito alla diffusione di un nuovo fenomeno di riciclaggio, che si asside sulla "polverizzazione dei contanti via internet"[2] e che consente di effettuare transazioni, da una parte all'altra del mondo, in modo sicuro e anonimo.

Si tratta di un fenomeno che prende il nome di "lavaggio virtuale" o "*cyberlaundering*" e che si realizza mediante l'impiego sistematico della valuta virtuale quale "mezzo elusivo della tracciabilità dei flussi di denaro"[3].

Tramite la criptovaluta si realizza, quindi, un'evoluzione delle tecniche di dissimulazione del capitale di origine illecita, che viene prontamente sfruttata dalla criminalità d'impresa.

Al fine di combattere il fenomeno del riciclaggio "via cripto" si ritiene indispensabile agire su un duplice fronte: da un lato, il versante repressivo, che impone l'utilizzo degli strumenti propri del diritto penale volti alla repressione del riciclaggio e dell'autoriciclaggio; dall'altro, il piano preventivo, sul presupposto che, per contrastare realmente simili fenomeni criminosi, sia essenziale non solo indagare sui casi di riciclaggio già in essere ma anche, e soprattutto, evitare che questi si verifichino.

In tale ottica appare opportuno intercettare, in via anticipata, le infiltrazioni criminali nel sistema economico, servendosi di presidi *ad hoc* e di una stretta collaborazione tra le varie autorità pubbliche, nazionali e internazionali, e gli operatori privati[4].

2. Le valute virtuali: inquadramento generale.

I rischi penali della valuta virtuale sembrano "intrinseci"[5] alla sua natura e, quindi, per comprendere e fronteggiare opportunamente le possibili implicazioni criminali che tale strumento di scambio comporta, si ritiene necessario un previo inquadramento delle valute virtuali.

Anzitutto, giova richiamare le fonti che, in assenza di una disciplina compiuta, contribuiscono alla delineazione delle caratteristiche fondamentali di tale valuta.

Va sottolineato come si tratti di un fenomeno oggetto di attenzione da più parti: da un lato, il Gruppo Finanziario d'Azione Internazionale (GAFI)[6], che ha elaborato un *report* sulle

[1] Sturzo (2018), p. 20.
[2] Simoncini (2015), p. 897.
[3] D'Agostino (2018), p. 2.
[4] La Rocca (2015), p. 202.
[5] Passarelli (2016), p. 1.
[6] Si tratta di un organismo inter-governativo composto da 36 membri in rappresentanza di Stati e organizzazioni regionali, che include come osservatori i principali centri finanziari internazionali, quali il Fondo Monetario Internazionale, la Banca Mondiale, la Banca Centrale

valute virtuali nel 2014[7], inteso come analisi specifica di un fenomeno più generale, quello dei nuovi e alternativi mezzi di pagamento, già affrontato a partire dal 2006; dall'altro, la Banca Centrale Europea (BCE) che, nel 2011, si è interessata alle interazioni che possono instaurarsi tra la valuta virtuale e l'economia reale, evidenziando anche i potenziali effetti di tali mezzi di pagamento sulla stabilità finanziaria e sulla politica monetaria[8].

Successivamente, un *focus* sulle *virtual currencies* è stato predisposto dall'*European Banking Authority*[9], con l'intento di fissare alcune definizioni utili allo sviluppo di un approccio normativo e di individuare i potenziali attori coinvolti.

Anche l'Italia si è, poi, interessata alla crescente diffusione delle valute virtuali e, in particolare, l'Unità di Informazione Finanziaria[10] ha predisposto una relazione sulle connotazioni peculiari delle criptovalute, mettendo in evidenza gli indicatori che giustificano il rischio di un utilizzo anomalo delle stesse[11].

Ma il punto di approdo nella disciplina delle valute virtuali, si rinviene nella Direttiva 2018/843/UE del Parlamento Europeo e del Consiglio[12], che rappresenta la prima regolamentazione a livello europeo delle valute virtuali.

Tuttavia, il legislatore nazionale, anticipando quanto poi sancito a livello unionale con tale V Direttiva, introduce una specifica definizione di valuta virtuale, con l'intento di garantire la certezza del diritto e di mettere ordine in una materia connotata da un profondo vuoto regolatorio.

Il d.lgs. 25 maggio 2017, n. 90[13], invero, all'art. 1, comma 2, lett. qq), statuisce che per "*valuta virtuale*" debba intendersi una "*rappresentazione digitale di valore, non emessa da una banca centrale o un'autorità pubblica, non necessariamente collegata ad una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente*".

Dal tenore letterale della norma si desume la qualificazione della valute virtuale nei termini di "contante digitale"[14], che si pone quale *tertium genus* tra la moneta fisica e quella elettronica e che assembla in sé i vantaggi di entrambe. Per vero, la valuta virtuale – e il *Bitcoin* in particolare – garantisce, da un lato, il generale accesso a chiunque, l'anonimato e la trasferibilità a basso rischio tipici della moneta fisica; dall'altro, la possibilità di effettuare pagamenti a distanza nonché la rapidità e i ridotti costi di transazione che caratterizzano la moneta elettronica[15].

In quanto rappresentazioni digitali di valore, esse non vengono emesse da banche centrali ma da soggetti che operano sul *web*, così da poter essere memorizzate sui propri dispositivi in appositi portafogli digitali (c.d. *e-wallets*) e, ove necessario, trasferite o negoziate elettronicamente[16].

A seconda del soggetto emittente, è possibile distinguere tra "valute centralizzate" e "valute decentralizzate"[17].

Europea e le Nazioni Unite; si occupa di sviluppare e promuovere strategie di contrasto al riciclaggio e al finanziamento del terrorismo, sviluppa *standard* riconosciuti a livello internazionale che, pur non producendo effetti giuridici immediati, influenzano comunque le politiche legislative degli Stati; approfondisce le nuove tecnologie e valuta i problemi strategici dei sistemi nazionali coinvolti. Per un approfondimento in tal senso, si veda l'indirizzo http://faft.gafi.org/pages/aboutus/membersandservers/ e La Rocca (2015), pp. 202- 203.

[7] FAFT, *Report, Virtual Currencies Key Definitions and Potential AML/CFT Risks*, June 2014, reperibile in http://www.faft-gafi.org/media/faft/documents/reports/virtual-currencies-key-definitions-and-potential-aml-cft-risks.pdf.

[8] ECB, *Report, Virtual currency schems, a further analysis*, February 2015, reperibile all'indirizzo: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[9] Il riferimento è a un *report* che prende il nome di "*EBA opinion on virtual currencies*" e che è stato pubblicato il 4 luglio 2014; è disponibile al seguente indirizzo: https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

[10] La UIF è stata istituita con il d.lgs. 21 novembre 2007, n. 231 (c.d. Decreto Antiriciclaggio), presso la Banca d'Italia ed è subentrata all'Ufficio Italiano dei Cambi (UIC); svolge un'attività di ricezione, analisi e comunicazione alle competenti autorità delle informazioni sulle ipotesi di riciclaggio o finanziamento al terrorismo. Per una disamina completa, La Rocca (2015), p. 203.

[11] UIF, *Utilizzo anomalo di valute virtuali,* rinvenibile sul sito Banca Italia all'indirizzo: https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Comunicazione_UIF_su_VV.pdf.

[12] Direttiva che modifica la precedente Direttiva 2015/849/UE relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le Direttive 2009/138/CE e 2013/36/UE, pubblicata in Gazzetta Ufficiale Europea il 19 giugno 2018.

[13] Si tratta di un decreto delegato, adottato in base alla legge 12 agosto 2016, n. 170, che è entrato in vigore il 4 luglio 2017 con il titolo di "*Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847*".

[14] L'espressione è di Passarelli (2016), p.2.

[15] Amato e Fantacci (2016), p. 4.

[16] Mancini (2015), p. 117.

[17] Tale distinzione è ampiamente presa in considerazione dal *Report* del GAFI prima citato e reperibile all'indirizzo http://www.faft-gafi.org/

Le prime sono emesse da un unico soggetto, il c.d. *administrator*, che definisce le regole di utilizzo delle valute, detiene il potere di ritirarle dal mercato e gestisce un registro pubblico in cui vengono annotate le diverse transazioni (c.d. *central payment ledger*). Esempio tipico di valuta a schema accentrato è rappresentato dal *Second Life Linden Dollar*.

Le valute decentralizzate, invece, non sono emesse da un soggetto specifico ma da più utenti operanti collettivamente attraverso la rete in modo non coordinato; in particolare, esse sono create in via diffusa per mezzo di un *software*, cioè di un sistema informatico *open source* che consente di trasferirle da un soggetto ad un altro. La sicurezza delle transazioni è assicurata dalla presenza di meccanismi di crittografia, in base ai quali si è soliti qualificare la valuta come "criptovaluta"[18].

Uno studio delle statistiche consente agevolmente di desumere come, attualmente, le valute virtuali più diffuse e utilizzate siano proprio quelle a schema decentrato[19], tra le quali è possibile annoverare il *Bitcoin*, il *Nextcoin*, il *Namecoin*.

Una seconda classificazione può essere effettuata in relazione al diverso grado di apertura delle valute virtuali nei confronti dell'economia reale, così distinguendo tra "valute virtuali convertibili" e "valute virtuali non convertibili" in moneta legale[20].

Le valute virtuali non convertibili, anche note come valute chiuse, sono quelle che non hanno alcun legame con l'economia reale; esse possono essere utilizzate solo per acquistare beni o servizi offerti all'interno della comunità virtuale, non potendo, almeno in teoria, essere scambiate al di fuori del sistema chiuso[21].

Le valute virtuali convertibili o aperte, invece, sono quelle rispetto alle quali è prevista la possibilità di una conversione in valuta avente corso legale; pur non trattandosi di una conversione garantita *ex lege*, si ritiene praticabile lo scambio nel rispetto delle regole di funzionamento proprie del tipo di valuta che, di regola, vengono cristallizzate nel *software* che le emette.

All'interno di tale categoria, è poi possibile tracciare un'ulteriore demarcazione, che consente di distinguere tra valute aperte con flussi unidirezionali e valute aperte con flussi bidirezionali. Le valute riconducibili al primo schema possono essere acquistate utilizzando la moneta legale ma non possono essere rivendute, così configurando una convertibilità limitata[22]; quelle rientranti nel secondo tipo, invece, possono essere scambiate con valuta reale ma è ammessa anche l'operazione inversa, permettendo l'acquisto tanto di beni digitali quanto di servizi reali.

A tale ultima fattispecie di valuta a convertibilità piena è possibile ascrivere il *Bitcoin*, che risulta essere la valuta virtuale più diffusa, con oltre il 90% della capitalizzazione del mercato.

3. Il *Bitcoin*, quale *species* della valuta virtuale: la natura decentralizzata e l'assenza di un ente di gestione o controllo.

Alla luce delle suesposte coordinate, si inizia a comprendere come le valute virtuali costituiscano un universo composito potenzialmente collegato al *cybercrime*; in tal senso, si ravvisa un rapporto di proporzionalità diretta[23] tra l'aumento di capitalizzazione del mercato delle valute virtuali e l'incremento di quel particolare tipo di reati che viene commesso per mezzo dei sistemi informatici.

Più specificamente, il *Bitcoin*[24] risulta essere la valuta maggiormente utilizzata per "ripulire"

media/faft/documents/reports/virtual-currencies-key-definitions-and-potential-aml-cft-risks.pdf.

[18] La Rocca (2015), p. 209; Di Vizio (2018), p. 34.

[19] Una delle piattaforme più aggiornate, sui cui è possibile consultare i dati in continua evoluzione, è rappresentata dal sito *web* http://coinmarketcap.com.

[20] Tale ripartizione è analizzata *funditus* in un *paper*, "*Virtual Currency Schemes*", pubblicato dalla Banca Centrale Europea che si rinviene al seguente indirizzo: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[21] Un tipico esempio è quello dei giochi *on-line*, le cui valute non possono essere convertite in *fiat currency*.

[22] Esempio tipico è quello dei *facebook credits*, acquistabili con denaro reale ma utilizzabili solamente per effettuare acquisti su *facebook*.

[23] IOCTA 2017, a cura *dell'Internet Cybercrime Centre* (EC3) costituito presso l'*Europol*. Questo rapporto, intitolato "*Internet Organised Crime Threat Assessment*" è rinvenibile all'indirizzo www.europol.europa.eu.

[24] Per una disamina completa di tale innovazione tecnologica si rinvia a Passarelli (2016), la quale evidenzia come la nascita del *Bitcoin* sia da ricondurre allo pseudonimo di Satoshi Nakamoto che, nel 2009, ha creato tale valuta con l'intento di differenziarla dalle altre esistenti. L'obiettivo era quella di istituire una valuta che non fosse solo in grado di trasferire potere d'acquisto ma anche di crearlo. Il *Bitcoin* si differenzia, poi, dalle monete per il suo essere un "attivo" senza comportare il "passivo" di nessun altro, così essendo più simile all'oro; e, come

i proventi illeciti derivanti dalla commissione di precedenti reati, sull'assunto che le caratteristiche di tale sistema rivelino una "ontologica natura dissimulatoria"[25].

Senza alcuna pretesa di completezza e solo con l'intento di esplicare la precedente asserzione, si evidenziano le connotazioni di tale *species* della valuta virtuale.

Come in parte accennato, si tratta di una criptovaluta dalla natura decentralizzata, pienamente convertibile, che si basa su una logica del "*peer to peer*"[26] (P2P, a rete paritaria), in base alla quale le transazioni avvengono tra gli utenti della rete in assenza di una intermediazione[27].

Si supera, quindi, la gestione centralizzata degli spostamenti patrimoniali tipica della moneta legale, che si caratterizza per la presenza di soggetti terzi, quali l'emittente o l'istituto bancario e finanziario, cui si attribuiscono i più svariati compiti, tra cui quelli di emettere la moneta, stabilirne le regole di utilizzo e svolgere attività di controllo o gestione.

Il sistema che ne deriva è qualificato da taluni come "*open source*"[28], poiché connotato dall'operare di soggetti indipendenti che pongono in essere operazioni ugualmente necessarie per il funzionamento dell'intero *network*[29], in assenza di un ente centralizzato o monopolistico in posizione preminente e gerarchicamente sovraordinata.

Ciò significa che non è più un unico soggetto esterno (es. l'istituto di credito) a dover verificare le transazioni; al contrario, in tale operazione di convalida e di autorizzazione sono coinvolti tutti gli utenti.

Più nel dettaglio, il sistema prevede che quando un soggetto effettui una transazione sia tenuto a trasmettere agli altri utenti una chiave criptata di accesso al conto; per poter autorizzare l'operazione, tale chiave deve essere decriptata. L'utente che, su base volontaria, riesce a decriptare la chiave di accesso prende il nome di "*miner*", cioè estrattore.

Il "*mining*" è, quindi, il processo di convalida delle transazioni e, al contempo, è anche l'unico modo per creare nuova valuta secondo lo schema *Bitcoin*; difatti, se è vero che i *miners* verificano le transazioni su iniziativa volontaria, è anche vero che il sistema prevede uno "stimolo premiale"[30], in conseguenza del quale si attribuiscono 50 *Bitcoin* di nuova creazione al *miner* che, per primo, risolve il problema matematico della chiave di accesso[31].

Alla luce di quanto asserito, quindi, appare evidente che i trasferimenti di *Bitcoin* avvengano senza l'intervento di un operatore professionale bancario o finanziario; di conseguenza, in tale sistema di valuta virtuale, manca il soggetto tenuto ad adempiere gli obblighi di identificazione della clientela e di segnalazione di operazioni eventualmente sospette[32].

È questo uno degli indicatori della pervasività delle criptovalute, che si prestano, per la propria natura, a superare le barriere della regolamentazione antiriciclaggio[33] e ad attrarre la criminalità organizzata, soprattutto quella di stampo mafioso[34].

A parere di alcuni, invero, la criminalità organizzata sembra essere alla costante ricerca di tecniche sempre più raffinate e nuove per delinquere impunemente e, in tal senso, pare essersi sviluppata una "capacità predittiva"[35], in virtù della quale si ravvisano notevoli applicazioni criminose delle *new technologies* prima ancora della loro implementazione sul mercato e della

l'oro si lega ad una scarsità naturale, anche il *Bitcoin* è connotato da una "scarsità artificiale", tale per cui la sua quantità risulta ancorata al protocollo informatico del *software* che lo emette.

[25] Tale espressione è di Sturzo (2018), p. 20.

[26] Vardi (2015), pag. 445.

[27] Un'analisi completa dello schema *Bitcoin* si trova in ECB, *Virtual currency schemes*, pubblicato ad ottobre 2012 in https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. In particolare, si veda pp. 21 ss.

[28] Passarelli (2016), p. 9.

[29] Accinni (2018), p. 4.

[30] L'espressione è di Accinni (2018), p. 3.

[31] ECB, *Virtual currency schemes*, p. 23. pubblicato ad ottobre 2012 in https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[32] Plantamura (2019), p. 883.

[33] Stokes (2012), p. 221.

[34] Plantamura (2019), pp. 875 ss., in cui l'Autore evidenzia come sia proprio la criminalità mafiosa a detenere un ruolo di rilievo nelle attività di riciclaggio, in base alla presenza di tre circostanze agevolative: l'ingente disponibilità di capitale liquido proveniente da attività delittuose, la volontà di infiltrarsi nei mercati legali (e tanto lo si desume anche dal tenore letterale dell'art. 416-*bis* c.p., in cui si fa riferimento al "controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici") e la necessità di minimizzare il c.d. *law enforcement risk*, cioè il rischio di essere arrestati e condannati. In senso analogo, Soldi (2011), p…… il quale asserisce che "il riciclaggio rappresenta uno sbocco assolutamente necessario delle attività illecite della criminalità organizzata: gli altissimi profitti del traffico degli stupefacenti, per esempio, possono essere utilmente impiegati solo in minima parte in analoghi comportamenti illeciti dovendo trovare, quindi, sbocco nel mercato legale in investimenti finanziari, imprenditoriali e commerciali formalmente leciti. Si può senza dubbio affermare che, ove non esistesse la possibilità di riciclare il denaro "sporco", verrebbe meno la stessa ragione di esistenza della criminalità organizzata, almeno nelle sue forme più complesse e più pericolose".

[35] Cucuzza (2007), pp. 350 ss.

loro regolamentazione ad opera del legislatore.

Tutto ciò premesso, occorre far chiarezza su quali possano essere gli altri soggetti coinvolti nelle transazioni digitali, delineando così le figure degli *users*, degli *exchangers*, dei *wallet providers*[36] e dei prestatori di servizi di *mixing*. Tale inquadramento sarà poi utile per riflettere sulla possibilità di configurare, in capo a taluni soggetti, una responsabilità a titolo di concorso nel delitto di riciclaggio con l'autore del reato presupposto o ancora una imputazione per auto-riciclaggio.

Gli *useres* sono definiti quali soggetti – persone fisiche o giuridiche – che ottengono il *Bitcoin* e lo utilizzano per acquistare beni o servizi reali e virtuali.

Gli *exchangers*, invece, sono coloro che svolgono un'attività di "ponte" tra il mondo della valuta virtuale e quello della moneta avente corso legale; più in particolare, tali soggetti offrono agli *users* un servizio di cambio valuta virtuale in moneta legale, al fine di ottenere una commissione.

Infine i *wallet providers*, noti anche come *custodians*, sono i soggetti che mettono a disposizione degli *users* un portafoglio elettronico mediante il quale detenere, conservare e trasferire i *Bitcoin* e conservare le chiavi private del conto.

Una considerazione particolare merita l'attività di *mixing*, della cui liceità si discute.

Come si avrà modo di precisare nel prosieguo, le transazioni virtuali sono annotate sulla *blockchain*, con la conseguenza che seppur anonime (*rectius*: pseudo-anonime), esse rimangono tracciabili.

Al fine di evitare la tracciabilità di attività sospette e di ridurre i "passaggi di mano" tra i vari portafogli digitali si può ricorrere ai servizi di *mixing*[37]. In particolare, gli utenti possono depositare un certo ammontare di *Bitcoin* su un conto di ingresso, per poi recuperarlo da un conto di uscita appositamente creato. Quindi, tramite l'attività del *mixer* sarà impossibile associare il *quantum* depositato inizialmente al *quantum* successivamente ritirato.

Tuttavia, è chiaro che un'attività di questo tipo si presti ad essere qualificata come "intrinsecamente illecita", potendo essere utilizzata per ostacolare l'identificazione della provenienza dei flussi di valuta virtuale[38]; ed è proprio la natura ontologicamente dissimulatoria di tale attività che induce a considerare la stessa come un indicatore relativo alla commissione di un potenziale reato di riciclaggio "via cripto".

3.1. *L'anonimato (*rectius*: pseudo-anonimato) delle transazioni* bitconiane.

L'analisi del sistema *Bitcoin* va completata ponendo evidenza ad un'altra connotazione peculiare, che contribuisce a rendere tale valuta virtuale "opaca" e intrinsecamente decettiva.

Muovendo dalla richiamata natura centralizzata delle transazioni, validate non da un unico gestore ma dagli stessi utenti, occorre sottolineare che tutte le operazioni *bitconiane* compiute nella rete sono annotate su un "libro contabile", cui ciascun *user* può accedere semplicemente dal proprio *computer*.

Tale libro contabile distribuito in rete (c.d. *distributed ledger*) prende il nome di *Blockchain*, in quanto consiste in una serie concatenata di blocchi; invero, le transazioni vengono raggruppate in blocchi e poi condivise. Grazie a tale sistema di "registrazione", le transazioni *bitconiane* sono pubbliche e accessibili costantemente a chiunque.

Tuttavia, a tale pubblicità in sé non corrisponde una trasparenza sui soggetti coinvolti, che rimangano quindi anonimi. In altri termini, le operazioni *bitconiane* sono tracciabili ma da questo non discende la sicura individuazione dell'identità degli *users* agenti; il dato che si rinviene ripercorrendo la catena delle transazioni, infatti, non è un nome ma una stringa alfanumerica, di complessa risoluzione e difficilmente riconducibile ad una persona fisica o giuridica.

Si parla di pesudo-anonimato proprio perché le Autorità possono pervenire alla chiave pubblica utilizzata dagli *users*, ma la difficoltà di decriptarla impedisce di risalire alla reale identità dell'ordinante e del ricevente. Lo pseudo-anonimato è, per giunta, agevolato dall'e-

[36] Tali definizioni si rinvengono nel *Report* dell'*European Banking Authority*, *Opinion on virtual currencies*, pp. 13-16, reperibile all'indirizzo https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.
[37] D'Agostino (2018), pp. 7-8.
[38] D'Agostino (2018), p. 8; Di Vizio (2018), p. 38.

sistenza di meccanismi informatici in grado di oscurare l'origine delle transazioni in *Bitcoin* (c.d. *anonymiser*), di collegare una transazione ad un indirizzo diverso da quello del soggetto ordinante (c.d. *mixer laundry service o tumbler*) o ancora di celare l'indirizzo IP dell'utente collegato alla rete (c.d. *Tor*)[39].

La situazione è resa, poi, ancora più complicata dalla circostanza che le transazioni possano coinvolgere anche soggetti residenti in Stati diversi, con la conseguenza di rendere il monitoraggio pressoché invano[40].

Proprio tali connotazioni della valuta virtuale giocano un ruolo determinante nelle possibili implicazioni criminali e risultano essere condizioni quantomeno predisponenti alle operazioni di riciclaggio[41]. Invero, potendo gli utenti trasferire denaro a velocità quasi istantanea senza controlli da parte di organismi centrali e con basse barriere all'ingresso nell'anonimato virtuale, in un sistema aggravato ulteriormente dai servizi di mixing, le *cryptocurrencies* ben potrebbero consentire ai riciclatori di spostare i fondi illeciti in maniera veloce, economica e discreta[42].

Alla luce delle descritte peculiarità della valuta virtuale e, in dettaglio, del *Bitcoin* si ravvisa un elevato rischio che tale mercato digitale divenga una sorta di "*cyber-heaven*"[43] per tutte le società che vogliano, con minor controlli, realizzare operazioni di riciclaggio.

4. Il *Cyberlaundering*.

Il *cyberlaundering* rappresenta un'evoluzione del tradizionale fenomeno di riciclaggio e si caratterizza per l'utilizzo della rete *Internet* e delle nuove tecnologie informatiche al fine di concretare una "ripulitura del denaro sporco"; in particolare, tale forma criminosa si asside sulla c.d. "polverizzazione dei contanti"[44] e sullo sfruttamento del *Computer* per la realizzazione di trasferimenti di quantità, anche ingenti, di denaro che derivino dal compimento di attività criminali[45].

La potenzialità offensiva del *cyberlaundering* emerge, in particolar modo, con riguardo alle operazioni telematiche aventi ad oggetto le valute virtuali, sulla scorta delle quali risulta possibile effettuare transazioni, da una parte all'altra del mondo, ad una velocità istantanea, senza barriere all'ingresso, in totale anonimato e in assenza di un controllo ad opera di istituti di vigilanza.

Definito anche come "lavaggio virtuale o cibernetico", il *cyberlaundering* costituisce una declinazione del più ampio fenomeno del *cybercrime*[46], intendendo con tale espressione il novero dei reati che si commettono o che possono commettersi in rete, nel *web* o nel c.d. *cyberspace*[47].

Una parte della dottrina[48] ritiene che, in tale categoria di reati cibernetici[49], possa tracciarsi una linea di demarcazione tra i reati in cui il *computer* e il sistema informatico rappresentano l'obiettivo delle attività criminali (c.d. *computer crimes*), i reati in cui il sistema informatico e la rete *Internet* rappresentano solo un aspetto possibile ed incidentale nella commissione dell'illecito, e i reati in cui il *computer* e le nuove tecnologie costituiscono proprio gli strumenti necessari per realizzare l'attività criminale (c.d. *computer facilitated crimes*).

In tale ultima categoria è possibile ascrivere il fenomeno di *cyberlaundering* poiché, come

[39] FAFT, *Report, Virtual Currencies Key Definitions and Potential AML/CFT Risks*, June 2014, reperibile in http://www.faft-gafi.org/media/faft/documents/reports/virtual-currencies-key-definitions-and-potential-aml-cft-risks.pdf.
[40] Sturzo (2018), p. 22.
[41] Di Vizio (2018), p. 57.
[42] Capaccioli (2015), p. 254.
[43] D'Agostino (2018), p. 4.
[44] Simoncini (2015), p. 1.
[45] Leslie (2014), p. 56.
[46] Per un approfondimento sul tema, Picotti (2008), pp. 700 ss; si veda anche *Comprensive Study on Cybercrime draft* – February 2013 (UNODC, New York), *Report* disponibile in https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
[47] Picotti (2019), p. 77.
[48] Flor (2012), p. 5.
[49] Il crescente sviluppo dei reati cibernetici, che vanno dai reati informatici inseriti nel codice penale (frodi, danneggiamenti, accessi abusivi) a quelli in senso ampio (quali il *cyberbullismo,* il *cyberterrorismo*, il *cyberlaundering*, la pedopornografia e l'adescamento di minori in rete), ha portato alla creazione di uno strumento interdisciplinare, all'interno del quale far convergere competenze accademiche, professionali, giudiziarie, tecniche, per poter meglio fronteggiare tali fenomeni criminali. Il riferimento è al c.d. "Osservatorio *Cybercrime*" disponibile al sito www.cybercrime.dgs.univr.it. Al proposito, si vedano le riflessioni di Picotti (2017), p. 322.

evidenziato, esso si asside sullo sfruttamento delle nuove tecnologie, dei *computer* e della rete per finalità criminose, nello specifico dissimulatorie e riciclatorie.

La minaccia del *cyberlaundering* appare particolarmente allarmante, proprio per il crescente utilizzo delle nuove tecnologie nelle varie fasi organizzative del riciclaggio e per i vantaggi che il "riciclatore professionista" può trarre dal ricorso alla rete *Internet* nello svolgimento delle attività criminali.

In particolare, va sottolineato come il *cyberspace* consenta all'autore del reato di beneficiare, oltre alla "dematerializzazione" delle risorse legate al contenuto digitale del denaro e alla "dispersione" dovuta alla difficoltà di individuare l'autore del reato[50], anche di una "delocalizzazione" o "deterritorializzazione" dell'utente, il quale, operando in rete, può essere virtualmente presente in più "spazi informatici" contemporaneamente[51].

A ciò consegue una considerazione in punto di giurisdizione, poiché il fatto illecito commesso in *Internet* non appare immediatamente riconducibile ad uno specifico *locus commisi delicti* e potrebbe involgere anche trasferimenti a livello sovranazionale, sfruttando così le condizioni più favorevoli dei Paesi privi di presidi antiriciclaggio[52]. Tale delocalizzazione, quindi, rende difficoltosa l'individuazione delle Autorità competenti, compresi i soggetti cui destinare eventuali richieste di natura cautelare o investigativa[53].

Alla luce delle considerazioni sinora svolte, pare potersi concludere che l'utilizzo delle nuove tecnologie nella commissione del riciclaggio determini una sorta di "schermo protettivo"[54], atto ad ostacolare non solo la conoscenza del fatto di reato ma anche la rintracciabilità dei soggetti coinvolti.

Tutto ciò premesso, deve evidenziarsi come il ricorso alle transazioni digitali incida sulle tradizionali fasi in cui il riciclaggio si articola.

Qualificato come processo teso a dissimulare l'origine illegale di un introito al fine di farlo apparire lecito[55], nella prassi esso si snoda in tre distinte fasi, ognuna delle quali può integrare da sé sola la fattispecie penalmente rilevante.

Come noto, infatti, la letteratura internazionale suddivide le operazioni di riciclaggio in tre momenti: il *Placement stage*, che consiste nel collocamento del denaro (dei beni o delle altre utilità) e nell'introduzione dei proventi illeciti nel mercato; il *Layering stage*, anche noto come stratificazione e lavaggio, che si basa sulle operazioni di copertura (tendenzialmente di natura finanziaria) della provenienza illecita in virtù delle quali si cerca di raggiungere una apparenza di legalità; l'*Integration stage*, che è l'ultima fase della filiera criminale e comporta la reintroduzione del capitale illecito[56], ormai "ripulito", nel circuito economico[57].

La rivoluzione informatica e le potenzialità delle piattaforme digitali hanno inciso su tutte le fasi, in taluni casi rendendone superflue alcune, ma l'impatto maggiore può registrarsi con riguardo al momento del *Placement stage*. Invero, se tradizionalmente il collocamento dei capitali di origine illecita richiede una azione fisica di spostamento materiale delle somme da ripulire[58], il *cyberlaundering* consente di elidere la movimentazione fisica dei flussi di denaro[59], poiché il contante da ripulire si trova già nel mondo virtuale e ha, quindi, una natura dematerializzata.

In sostanza, con il *cyberlaundering* si elimina uno dei maggiori rischi insiti nel riciclaggio, non essendo più necessario il contatto materiale tra il contante e l'autore del reato. Di conseguenza, l'incidenza dello spazio virtuale nella commissione dei fatti di riciclaggio può comportare anche la potenziale eliminazione delle ultime due fasi del processo criminoso nella particolare forma del *cyberlaundering* integrale.

[50] Simoncini (2015), p. 897.
[51] Flor (2019), p. 143.
[52] Per un approfondimento in tal senso, Bordot (2016)
[53] Accinni (2018), pp. 13-14.
[54] Accinni (2018), p. 1.
[55] Pecorella (1989), p. 366 ss.
[56] Soldi (2011), il quale evidenzia come il modello a ciclo del riciclaggio si articola sul seguente passaggio: dall'economia illegale si transita nell'economia legale, per poi passare ancora all'economia illegale. Tanto si spiega in relazione alla circostanza che gran parte del denaro ripulito torna a rifornire le attività criminali, così partecipando alla produzione di altri fondi che, a loro volta, dovranno essere ripuliti. La restante parte di denaro, invece, rimane nell'economia lecita.
[57] Castaldo (2013), pp. 225 ss.; Masciandaro (2012), pp. 15 ss.
[58] Simoncini (2015), p. 899.
[59] In ragione di tale possibilità, il *cyberlaundering* è definito quale "riciclaggio del terzo millennio" da Rapetto (1999), p. 3, che evidenzia come le caratteristiche dei nuovi mezzi di pagamento siano in grado di superare uno dei più rilevanti problemi in tema di riciclaggio, quello relativo alla movimentazione fisica di grandi quantità di denaro.

Sul punto, pare opportuno richiamare la distinzione tra il *cyberlaundering* strumentale, che si caratterizza per la presenza, quantomeno iniziale, del denaro contante, e il *cyberlaundering* integrale, connotato dalla circostanza che il denaro sporco da ripulire abbia sin dall'inizio uno "stato digitale"[60].

Questa differenziazione si riverbera sulla struttura dei due processi criminosi perché, mentre nel riciclaggio digitale strumentale l'apporto tecnologico si inserisce nella filiera criminale agevolando qualche passaggio, nel riciclaggio digitale integrale il procedimento di *laundering* si realizza con un'unica operazione, effettuata mediante transazioni economico-finanziarie che avvengono integralmente *on-line*, così riducendo anche i rischi connessi a tale attività[61].

La fase di *placement stage*, in tale ipotesi, apre e chiude il processo di "ripulitura" e assorbe, quindi, le due fasi successive del lavaggio e del reimpiego del denaro sporco digitale; proprio per la potenziale pervasività di un simile fenomeno, si ritiene che il *cyberlaundering* integrale rappresenti l'ultima vera frontiera del riciclaggio.

Così delineate le caratteristiche essenziali di tale fenomeno criminoso, si deve precisare che, nel nostro ordinamento, non si rinviene una fattispecie legale che tipizzi il fenomeno in senso unitario e specifico, a differenza di quanto avviene con riguardo ad alcuni *computer crimes*.

La legge 23 dicembre 1993, n. 547, invero, nel tentativo di mettere ordine nella materia dei reati informatici, introduceva nel codice penale alcune fattispecie incriminatrici *ad hoc*, quali il danneggiamento informatico (art. 635-*bis*), la diffusione di programmi *malware* potenzialmente nocivi (art. 615-*quinquies*), la violazione del domicilio informatico (art. 615-*ter*).

Tuttavia, per il riciclaggio digitale manca un intervento legislativo simile e questo pone il problema di verificare quale sia lo spazio entro cui il diritto penale possa già attualmente fronteggiare i profili più critici di tale fenomeno e soddisfare le esigenze di protezione individuale e collettiva che si impongono.

Ebbene, pare utile ribadire che l'utilizzo del *web* nella commissione del reato di riciclaggio possa rilevare come mera modalità della condotta – strumentale o integrale, a seconda dei casi –, con la conseguenza di una incidenza solo ai sensi dell'art. 133 c.p. in sede di commisurazione della pena[62]. Resta da verificare e valutare l'astratta applicabilità delle fattispecie incriminatrici vigenti nel nostro ordinamento (artt. 648-*bis* e 648-*ter*1 c.p.) anche alle ipotesi di riciclaggio *via cripto*, senza che ciò determini una illecita estensione della punibilità in violazione del principio di legalità sub-specie di divieto di analogia[63].

5. La sussumibilità nelle fattispecie codicistiche: alcune preliminari considerazioni.

De iure condito si ritiene che la via maggiormente efficace per contrastare il fenomeno del *cyberlaurndering* sia quella di ricorrere alle fattispecie codicistiche di cui agli artt. 648-*bis* e 648-*ter*1 c.p. ma, prima di esaminare *funditus* i principali dubbi ermeneutici che hanno impegnato (e impegnano) la dottrina, pare utile far precedere l'analisi di dettaglio da alcune considerazioni di carattere generale sulle fattispecie richiamate.

Il reato di riciclaggio, che originariamente era stato inserito nel codice penale[64] con la rubrica di "sostituzione di denaro o valori provenienti da rapina aggravata, estorsione aggravata o sequestro a scopo di estorsione", è stato oggetto di numerosi interventi legislativi[65] che hanno condotto alla formulazione attuale, rubricata "riciclaggio", che si caratterizza per il superamento della tassativa indicazione dei reati da cui derivano i proventi illeciti e per la *ratio* di tutela volta a impedire la re-immissione del capitale illegale, ormai ripulito, nel circuito economico – produttivo legale[66].

[60] Simoncini (2015), p. 901.
[61] Alcini (2018), p. 448
[62] Plantamura (2019), p. 871.
[63] Sturzo (2018), p. 23.
[64] Il riferimento è alla legge 18 marzo 1978, n. 191.
[65] Si richiama la legge 19 marzo 1990, n. 55, la successiva riforma ad opera dell'art. 4, legge 9 agosto 1993, n. 328. Per un maggior approfondimento, Mazzacuva (1991), p. 501 ss.
[66] Fiandaca e Musco (2015), p.260. In senso analogo, Mezzetti (2013), p. 630.

Come si accennava, le condotte incriminate sono quelle di sostituzione[67], trasferimento[68] o compimento di altre operazioni[69], che assumono rilevanza penale quando siano idonee ad ostacolare l'identificazione dell'originaria provenienza delittuosa dei beni[70]. Sul punto, giova precisare che la giurisprudenza di legittimità[71] ha ritenuto sussistente l'ostacolo non a fronte di un impedimento insormontabile quanto piuttosto in presenza di una maggiore difficoltà nell'accertamento; di conseguenza, la natura dissimulatoria delle condotte sussiste anche quando l'accertamento si riveli possibile ma ne risulti appesantito l'*iter*[72].

Tuttavia, in virtù della clausola di riserva posta in apertura dell'art. 648-*bis* c.p., originariamente non risultava punibile la condotta decettiva realizzata dall'autore o dal concorrente nel reato presupposto, sull'assunto che tali operazioni dissumulative rappresentassero la "normale" prosecuzione del reato e che, quindi, andassero ad integrare una sorta di *post factum* non punibile[73].

Sulla spinta di impulsi internazionali ed europei, tale "privilegio di autoriciclaggio" viene espunto dal nostro ordinamento con l'art. 3 della legge 15 dicembre 2014, n. 186 che, anziché disporre una interpolazione del testo dell'art. 648-*bis* c.p. volta ad eliminare la clausola di riserva, introduce una fattispecie *ad hoc* con l'art. 648-*ter*1 c.p.

Una prima analisi testuale del dato normativo consente di evidenziare come il delitto di autoriciclaggio[74] sia strutturato in una sorta di crasi tra gli artt. 648-*bis* e 648-*ter* c.p., in virtù della quale si mutua dal riciclaggio la decettività della condotta e dal reimpiego la condotta di impiego[75].

Ciò significa che, per la configurazione del reato, si richiede sia la destinazione degli impeghi in un'attività economica, finanziaria, imprenditoriale o speculativa, sia la modalità della condotta "concretamente"[76] idonea ad ostacolare l'identificazione della provenienza delittuosa.

Terreno fertile per critiche e orientamenti contrastanti in dottrina sembra essere quello relativo al bene giuridico[77] tutelato dall'art. 648-*ter*1 c.p.

Muovendo dal dato testuale, si evince la rilevanza di un doppio bene giuridico[78]: da un lato, l'ordine economico potenzialmente alterato dalla destinazione dei proventi illeciti in una delle attività indicate; dall'altro, l'amministrazione della giustizia, lesa dalle condotte che ostacolano la tracciabilità della provenienza dei beni[79].

Ciò premesso, occorre precisare che una reale comprensione dell'interesse tutelato dalla nuova disposizione incriminatrice presuppone un'analisi del dibattito sull'individuazione dei beni giuridici tutelati dal riciclaggio e dal reimpiego; una conferma in tal senso si trae dalla circostanza che il delitto di cui all'art. 648-*ter*1 c.p. si pone come fattispecie ibrida, che ingloba in sé le caratteristiche delle due norme incriminatrici che la precedono.

Al proposito, se è pacifico che la norma sull'impiego di cui all'art. 648-*ter* c.p. tuteli l'ordine economico, sull'assunto che l'investimento di ingenti proventi da parte delle imprese criminali costituisca una turbativa del mercato, più "sfuggevole"[80] appare il bene giuridico protetto con la disposizione di cui all'art. 648-*bis* c.p.

[67] Zanchetti (1997), pp. 208 ss, che descrive la "sostituzione" come quell'insieme di operazioni (bancarie, finanziarie, commerciali) finalizzate a separare il compendio criminoso dal reato presupposto, così eliminando il collegamento con esso.
[68] Soldi (2011), il quale definisce il "trasferimento" come uno spostamento di beni da un soggetto ad un altro, al fine di far perdere le tracce della provenienza e della effettiva destinazione; si tratta di una attività che differisce dalla sostituzione in virtù del fatto che i proventi del reato vengono spostati e trasferiti nella loro composizione qualitativa e quantitativa.
[69] Soldi (2011), si tratta di una clausola di chiusura tesa ad assicurare la punibilità di qualsiasi operazione, diversa dalla sostituzione e dal trasferimento, idonea ad ostacolare l'identificazione del denaro, dei beni o delle utilità di provenienza illecita.
[70] Dell'Osso (2017), p. 110 specifica che il reato di riciclaggio viene qualificato come reato a pericolo concreto, a forma sostanzialmente libera, con la precisazione che il pericolo (cioè l'attitudine dissimulatoria delle condotte) costituisce un elemento legale della fattispecie che, di volta in volta, deve essere accertato dal giudice.
[71] Cass. pen., Sez. II, 12 gennaio 2006, n. 2818; Cass. pen., Sez. II, 9 marzo 2015, n. 26208.
[72] Mezzetti (2013), p. 655.
[73] *Ex multis*, Castaldo e Naddeo (2010), pp. 92 ss.; Seminara (2005), pp. 236 ss.; Manes (2004), pp. 75 ss.; Bricchetti (2014), pp. 684 ss.
[74] Per un maggiore approfondimento si veda Gullo (2015),pp. 275- 288 e Gullo (2017), pp. 483- 489.
[75] Gullo (2015), p. 281.
[76] Si ritiene che l'introduzione espressa di una idoneità "concreta" debba essere intesa come monito per l'interprete ad evitare interpretazioni formalistiche che portino a sanzionare comportamenti astratti e scarsamente ostacolanti; si richiede una verifica concreta del giudice, attenta al principio di offensività. In tal senso Fiandaca e Musco (2015), p. 274. Specifica ulteriormente Ciraulo (2016), p. 10 che la concreta idoneità del mezzo costituisce il *quid pluris* rispetto ad una condotta di mero e automatico uso del provento illecito.
[77] In via generale Paliero (2012), pp. 102 ss.
[78] In tal senso Ciraulo (2016), p. 9.
[79] In senso parzialmente difforme Seminara (2015), p. 1638, il quale sostiene che l'offensività dell'autoriciclaggio sia mutuata essenzialmente dalla norma sul riciclaggio, ritenendo l'offesa all'ordine economico, insita nel reimpiego, solo eventuale.
[80] Manes (2006), p. 5230.

Sul punto si sono succeduti diversi indirizzi dottrinali, tesi a valorizzare interessi anche eterogenei tra loro. Anzitutto, muovendo da una interpretazione sistematica, attenta alla collocazione della norma incriminatrice nell'ambito dei reati contro il patrimonio, si è ritenuto di individuare il disvalore del riciclaggio nell'offesa patrimoniale, sul presupposto che tale condotta di "ripulitura" vada a consolidare e "perpetrare"[81] la lesione posta in essere dal c. *predicate crime*[82].

Tuttavia, ritenendo tale impostazione restrittiva e, in parte, lesiva del *ne bis in idem* sostanziale, si è imposto un secondo orientamento che, nel tentativo di valorizzare l'autonomia della fattispecie di riciclaggio rispetto al reato presupposto, abbraccia una concezione del "patrimonio" tutelato in un'ottica generale e astratta, non più individualistica[83]. Si riflette, cioè, sull'incidenza del riciclaggio sull'economia legale e sui pregiudizi che da esso derivano nel sistema economico e nel regime di concorrenza[84].

Tra i beni tutelati dalla norma incriminatrice, assieme all'ordine economico, si considera poi primaria la tutela dell'amministrazione della giustizia; in particolare, si evidenzia la natura di reato- ostacolo del riciclaggio, poiché le condotte incriminate sono orientate alla dissimulazione della provenienza delittuosa dei beni e, quindi, questo finisce per incidere sull'attività di accertamento dei reati e di individuazione dei colpevoli condotta dall'Autorità giudiziaria[85].

Alla luce delle considerazioni svolte si conclude in favore della natura plurioffensiva del delitto di riciclaggio e, conseguentemente, di quello di autoriciclaggio.

In sintesi, la nuova incriminazione sembra porsi a tutela della tracciabilità dei flussi finanziari[86], dell'amministrazione della giustizia e dell'ordine economico[87].

Le considerazioni sinora svolte sul profilo offensivo sembrano utili per comprendere, nel prosieguo della trattazione, le questioni applicative che si pongono in relazione al *cyberlaundering* e al *cyber-selflaundering*, con particolare riguardo al meccanismo di concorso di reati nel riciclaggio o nell'autoriciclaggio.

5.1. *La sussumibilità nelle fattispecie codicistiche: una strada percorribile? Riflessioni sull'oggetto del reato.*

Il primo nodo problematico che l'interprete deve affrontare nel valutare la riconducibilità del fenomeno di *cyberlaundering* nelle fattispecie incriminatrici di riciclaggio e autoriciclaggio attiene ad una questione di compatibilità c.d. oggettiva.

Muovendo dalla considerazione che le operazioni compiute sulle piattaforme digitali possano essere ricomprese senza difficoltà in uno dei tre modelli fattuali della condotta (sostituzione, trasferimento, compimento di altre attività), occorre riflettere sulla sussumibilità della valuta virtuale nell'oggetto materiale descritto dalla norma. Più in dettaglio, ci si deve chiedere se le valute virtuali e, nello specifico, i *Bitcoin* possano essere qualificati come "denaro, beni o altra utilità".

In primo luogo, oggetto materiale del reato può essere il "denaro" o gli strumenti ad esso assimilabili, in quanto impiegati come mezzo di adempimento delle obbligazioni, quali gli assegni postali o bancari, i vaglia postali, le carte di credito.

Sul punto, si deve evidenziare come la dottrina prevalente tenda ad escludere l'assimilabilità delle valute virtuali alla moneta legale[88] e, quindi, al denaro. Invero, secondo la teoria statuale della moneta[89], si può considerare denaro solo la moneta regolamentata, provvista di corso legale (con conseguente potere liberatorio e solutorio delle obbligazioni pecuniarie) e

[81] L'espressione è di Zanchetti (1997), p. 390.
[82] Tale tesi si sviluppava in un contesto normativo in cui i reati presupposto erano, quasi esclusivamente, reati contro il patrimonio. Si veda Brunelli (2015), p. 90.
[83] Dell'Osso (2017), p. 73.
[84] Cocco (2011), p. 1467 ss.
[85] Cerqua (2008)., pp. 66- 67.
[86] Dell'Osso (2017), p. 181.
[87] Si sanzionano, infatti tutti i comportamenti che innescano meccanismi distorsivi dei sistemi economici e i turbamenti del mercato connessi alle infiltrazioni di denaro illecito,
[88] Di Vizio (2018), p. 41. Anche l'EBA ha precisato di non considerare la valuta virtuale come una forma autentica di moneta, come si evince da *EBA opinion on virtual currencies*", disponibile al seguente indirizzo: https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.
[89] Per un quadro sulle varie teorie della moneta, Gasparri (2015), pp. 417 ss.

di corso forzoso (con derivata impossibilità di essere rifiutata come mezzo di pagamento)[90].

Quindi, è garantita dalla legge solo la moneta espressione della sovranità statale, la cui emissione è, di regola, riservata alle banche centrali. Come già evidenziato, invece, le valute virtuali sono generate da soggetti privati, in assenza di un'autorità centralizzata o monopolistica, e il loro utilizzo come mezzo solutorio non è imposto dalla legge ma solo da un eventuale e preventivo accordo tra le parti del rapporto obbligatorio[91].

Dal tenore testuale degli artt. 648-*bis* e 648-*ter*1, si evince, poi, che oggetto materiale del reato possa essere anche un "bene", proveniente da qualsiasi delitto non colposo. Quindi, esclusa la possibilità di ricondurre le valute virtuali nella nozione di "denaro", ci si deve chiedere se queste possano essere sussunte nella più ampia nozione di "bene".

L'addentellato normativo che consente di chiarire la portata di tale sintagma si rinviene nell'art. 810 c.c., a tenore del quale "sono beni le cose che possono formare oggetto di diritti".

In virtù di una interpretazione estensiva, pare possibile ricomprendere nel novero dei "beni" sia la *res* materiale che quella immateriale, abbracciando così una concezione di bene in senso giuridico[92] (in difformità dalla concezione di bene in senso corporale); di conseguenza, pare possibile considerare la valuta virtuale come bene *ex* art. 810 c.c., sull'assunto che si tratti una tipologia di bene immateriale[93].

Tuttavia, una parte della dottrina si pone in senso critico rispetto alla possibilità di considerare il *Bitcoin* come rientrante nella nozione civilistica di "bene", argomentando che i beni immateriali costituiscano, nel nostro ordinamento, un *numerus clausus*[94].

Di conseguenza il principio di stretta tipicità, alla stregua del quale i diritti sui beni immateriali esistono in quanto ci sia una norma che li preveda, porterebbe a disconoscere un diritto di esclusiva sulle valute virtuali.

Ma, anche a voler aderire a tale restrittiva impostazione, si deve comunque ricordare che le norme incriminatrici in esame, proprio al fine di evitare indebite esclusioni dal raggio applicativo della disposizione, riconoscono quale oggetto materiale del reato anche ogni "altra utilità"[95].

Con tale locuzione, il legislatore ha inserito una sorta di clausola di chiusura, tesa a ricomprendere qualunque vantaggio che derivi dal compimento del reato presupposto. In tale ottica, deve intendersi ogni valore economicamente apprezzabile e tutto ciò che rappresenti il "frutto dell'attività criminosa precedente"[96]; di conseguenza, non pare contestabile la sussumibilità della valuta virtuale, quale prodotto del reato, in tale ampia nozione di utilità[97].

Alla luce delle considerazioni sinora svolte, sembra possibile concludere nel senso di una sanzionabilità *ex* artt. 648-*bis* e 648-*ter*1 c.p. sia di quanti, dopo aver commesso un reato presupposto, trasferiscano i proventi virtuali o reali ad un terzo affinché questi, tramite la rete, ponga in essere operazioni di *cyberlaundering*, sia di quanti adottino personalmente condotte decettive e dissimulatorie, mediante l'impiego in attività economiche, finanziarie, imprenditoriali o speculative.

5.2. *La sussumibilità nelle fattispecie codicistiche: il profilo soggettivo e i problemi in tema di concorso nell'autoriciclaggio.*

Alla luce delle suesposte coordinate ermeneutiche, pare opportuno precisare che la sus-

[90] Tuttavia, secondo Vardi (2015), pp. 446- 447, pur non potendo qualificare i *Bitcoin* come moneta legale, ad essi può essere riconosciuta una "funzione monetaria", che risponde alle tre caratteristiche tipiche di riserva di valore, unità di conto e mezzo di scambio; in senso contrario, Bocchini (2017), p. 29 ss , secondo cui il *Bitcoin* non riuscirebbe ad assolvere neppure questi ruoli, in quanto la funzione di riserva di valore sarebbe impedita dall'estrema volatilità della valuta virtuale, la funzione di mezzo di scambio sarebbe minata dalla circostanza di non essere imposta dallo Stato e di dipendere da un previo accordo delle parti, la funzione di unità di conto sarebbe pregiudicata dalle incertezze insite nel mercato dei cambi virtuale- reale.

[91] Mancini (2015), p. 124.

[92] Gambaro (2012), p. 275.

[93] Di Vizio (2018), p. 44.

[94] Zeno e Zenovich (1989), p. 460.

[95] Tale locuzione viene intesa in senso ampio, così da ricomprendere non solo l'incremento del patrimonio ma anche il mancato decremento e, quindi, anche il risparmio di spesa che un soggetto ottiene quando non procede al pagamento delle imposte dovute. *Ex plurimis*, Cass. pen., Sez. III, 26 maggio 2010, n. 25890 e Cass. pen. Sez. VI, 23 aprile 2010, n. 25807.

[96] In tal senso si pone anche la giurisprudenza di legittimità, Cass. pen., Sez. II, 17 gennaio 2012, n. 6061.

[97] Di Vizio (2018), p. 57. In senso analogo, Capaccioli (2015), p. 252.

sumibilità nell'art. 648-*bis* o 648-*ter*1 c.p. di una condotta di *cyberlaundering* presuppone una previa valutazione soggettiva, tesa a chiarire il ruolo del soggetto agente e a comprendere se questo abbia o meno concorso nel reato base. Invero, il delitto di autoriciclaggio, in disparte la condotta di impiego nel mercato economico, sembra costruito sulla falsariga del reato di riciclaggio, distinguendosi da questo per l'identità del soggetto attivo.

Il legislatore del 2014 sembra, cioè, tracciare una linea di demarcazione tra la figura del "riciclatore professionista"[98] e quella dell'autoriciclatore. Nel primo caso, si ha un soggetto terzo, non partecipe del reato presupposto, che – in qualità di intermediario – pone in essere delle operazioni di ripulitura del denaro volte a ostacolare la tracciabilità della provenienza delittuosa; nel secondo caso, lo stesso autore o concorrente nel reato base impiega i proventi che ne derivano nel circuito economico, creando un ostacolo concreto alla loro identificazione[99].

In altri termini, le disposizioni di cui agli artt. 648-*bis* e 648-*ter*1 c.p. paiono caratterizzarsi per una "soggettività differenziata alternativa", in virtù della quale deve verificarsi, di volta in volta, se il fatto ipotizzato integri il reato di riciclaggio o di autoriciclaggio, a seconda che il soggetto riciclatore sia lo stesso autore del reato presupposto o un soggetto terzo che, nel caso del *cyberlaundering*, può essere il cambia valute virtuale (*exchanger*), il *wallet provider* (depositario *on-line* di valute virtuali), l'*host provider* (colui che offre la piattaforma su cui effettuare lo scambio) o il *miner* (l'utente terzo che convalidano la transazione illecita), di cui si è trattato in precedenza.

Va precisato che la condotta dissimulatoria *on-line* posta in essere dall'autore del reato o da un soggetto concorrente, riconducibile al nuovo art. 648-*ter*1 c.p., può derivare tanto da una persona fisica quanto da una persona giuridica. Difatti, la legge 15 dicembre 2014, n. 186, oltre ad introdurre nel codice penale una fattispecie *ad hoc*, realizza una interpolazione dell'art. 25-*octies* del d.lgs. 8 giugno 2001, n. 231, includendo il nuovo delitto di autoriciclaggio nel novero dei reati presupposti che determinano la responsabilità dell'ente[100].

Così chiarita la distinzione tra *cyberlaundering* e *self-cyberlaundering*, con la conseguente riconducibilità ad una diversa fattispecie codicistica, occorre esaminare la problematica questione di una realizzazione plurisoggettiva dell'autoriciclaggio.

Ci si interroga, cioè, sulla qualificazione giuridica da attribuire alla condotta posta in essere da un soggetto *extraneus* (colui che non abbia commesso il delitto non colposo presupposto e che non vi abbia neppure concorso), che abbia fornito un contributo causalmente rilevante[101] alla condotta di autoriciclaggio compiuta dal soggetto *intraneus* (cioè colui che abbia commesso o abbia concorso a commettere il c.d. *predicate crime*).

Si pensi al caso in cui un *exchanger* o un *miner* ponga in essere, assieme all'autore del delitto base, una condotta di impiego dei proventi nel circuito economico con lo scopo di dissimulare la loro provenienza delittuosa; in tale ipotesi di realizzazione pluripersonale di fatti riconducibili all'autoriciclaggio, ci si chiede se l'*extraneus* (i.d. l'*exchanger* o il *miner*) debba rispondere a titolo di concorso nel delitto di autoriciclaggio o se, viceversa, debba essere sanzionato per aver commesso il reato di riciclaggio in via monosoggettiva.

La scelta dell'una o dell'altra opzione, lungi dall'essere una questione meramente teorica, porta con sé una notevole rilevanza applicativa, a causa della diversa cornice edittale che connota le due fattispecie in esame, sia sul versante della pena base che su quello delle circostanze[102].

Una prima impostazione si asside sulla preliminare considerazione che il delitto di autoriciclaggio debba essere qualificato come "reato proprio" o a "soggettività qualificata", potendo essere commesso non da qualsiasivoglia soggetto ma solo da colui che sia autore (o con-

[98] L'espressione è di Simoncini (2015), p. 913.

[99] Sgubbi (2015), p. 137 ss., pone in evidenza una ulteriore distinzione tra il reato di riciclaggio e quello di autoriciclaggio: oltre al profilo soggettivo, si sottolinea come il riciclaggio presupponga il compimento di attività "astrattamente" idonee ad ostacolare la tracciabilità della provenienza criminosa, mentre l'incriminazione di nuovo conio richiede espressamente una attività "concretamente" atta ad ostacolare tale identificazione.

[100] Anche l'ente è, quindi, chiamato a rispondere del delitto di autoriciclaggio quando un soggetto apicale o subordinato all'altrui direzione o vigilanza, nell'interesse o a vantaggio dell'ente, compia dapprima un delitto non colposo da cui derivino dei proventi e poi impieghi gli stessi in un'attività economica, finanziaria, imprenditoriale o speculativa, così da frapporre un concreto ostacolo alla tracciabilità della provenienza delittuosa, in presenza, beninteso, di una colpa c.d. di organizzazione dell'ente. Sul punto si veda Gullo (2018), pp. 3017- 3045.

[101] Si tratta di un'ipotesi nient'affatto infrequente nella prassi applicativa; anzi, l'esperienza dimostra che maggiori sono le quantità di profitto da dissimulare, maggiore è la tendenza a ricorrere alla professionalità di soggetti terzi. Si veda Dell'Osso (2017), p. 216.

[102] Gullo (2017), p. 487 evidenzia come il quadro edittale dell'autoriciclaggio sia più contenuto rispetto a quello del riciclaggio e del reimpiego.

corrente) del precedente reato[103]. Invero, a dispetto dell'utilizzo del sintagma "chiunque", la formulazione della norma induce a considerare come soggetto attivo solo colui che abbia una "relazione" (autore o concorrente) con la commissione di un precedente delitto non colposo.

Ne consegue che il terzo privo della qualifica soggettiva tipica, il quale abbia contribuito alla dissimulazione dei proventi assieme all'*intraneus*, possa rispondere di concorso nel reato di autoriciclaggio[104], mediante il ricorso alle norme di cui agli artt. 110 e 117 c.p., a seconda che il terzo *extraneus* abbia o meno consapevolezza della qualifica dell'*intraneus*.

Aderendo a tale indirizzo, tuttavia, si assisterebbe ad una erosione dell'ambito applicativo della fattispecie di riciclaggio e, al contempo, si determinerebbe un alleggerimento della risposta sanzionatoria anche nei confronti del terzo, sfruttando una norma che era stata invece coniata per assicurare la punibilità dell'autoriciclatore e non certo per attenuare le pene del riciclatore[105].

Onde evitare tale esito irragionevole, pare potersi sostenere una diversa impostazione, di recente corroborata anche dalla giurisprudenza di legittimità[106] e basata sull'idea di una differenziazione dei titoli di reato.

In particolare, si ritiene che il soggetto terzo il quale, non avendo concorso nel reato base, ponga in essere la condotta tipica di autoriciclaggio o contribuisca alla sua realizzazione da parte dell'autore del reato, debba rispondere di riciclaggio e non di concorso nel delitto di autoriciclaggio, potendo quest'ultimo configurarsi solo in capo *all'intraneus*.

Ne consegue che, mentre *l'intraneus*[107] risponderà di autoriciclaggio, la condotta dell'extraneus non potrà che essere ricondotta alla più grave fattispecie riciclatoria prevista e punita dall'art. 648-bis c.p.

Le considerazioni sinora svolte consentono di concludere nel senso di una responsabilità penale *sub-specie* di riciclaggio per quei soggetti che, svolgendo un'attività di cambia valute, di deposito *on-line* crittografato o di validazione delle transazioni, forniscano un contributo causale per la commissione della condotta autoriciclatoria ad opera dell'autore del c.d. *predicate crime*. Pur tuttavia, deve precisarsi che la sanzionabilità degli stessi resta pur sempre condizionata ad una previa verifica in tema di elemento soggettivo.

Sul punto, la giurisprudenza pare pacifica nel ritenere che tali soggetti terzi possano rispondere per la commissione di un reato di riciclaggio o per aver concorso nell'altrui riciclaggio quando sia ravvisabile quanto meno il dolo eventuale, ovvero la rappresentazione del rischio che il denaro o la valuta virtuale ricevuti abbiano una provenienza delittuosa[108].

Ricalcando i principi sostenuti in tema di ricettazione, si specifica poi che l'accettazione del rischio della dubbia provenienza dei proventi possa desumersi da "qualsiasi elemento"[109], ma non implica la precisa e completa conoscenza delle circostanze di tempo, di modo e di luogo del reato fonte[110].

Così intesi i requisiti relativi all'elemento soggettivo, si devono richiamare le caratteristiche peculiari delle valute virtuali di cui si è ampiamente dato atto: la volatilità, la natura intrinsecamente opaca e dissimulatoria delle criptovalute, l'anonimato (*rectius*: pseudo-anonimato) delle transazioni sembrano inevitabilmente configurare in capo agli operatori digitali, quali *exchangers*, *miners* e *mixers*, quanto meno la possibilità della provenienza delittuosa dei proventi ricevuti o impiegati[111].

Tuttavia, sebbene questa sia la tesi più diffusa in dottrina, non manca chi evidenzia che far rispondere gli operatori virtuali a titolo di dolo eventuale, per essersi rappresentati la possibilità della illecita provenienza e per aver agito accettandone il relativo rischio, comporterebbe una sorta di "incriminazione *ad infinitum*"[112]. Il sistema virtuale, invero, è strutturato su base paritaria, con la conseguenza che gli utenti siano legati tra loro da un rapporto fiduciario, in assenza di un ente monopolistico o centralizzato che vigili sul loro operato; così facendo, cioè, si correrebbe il rischio di alterare lo stesso funzionamento del mondo virtuale.

[103] Fiandaca e Musco (2015), pp. 272 ss.
[104] Troyer e Cavallini (2015), p. 104.
[105] Gullo (2018), p. 264.
[106] Cass. pen., Sez. II, 17 gennaio 2018, n. 17235.
[107] Cass. pen., Sez. II, 17 gennaio 2018, n. 17235.
[108] Cass. pen., Sez. V, 17 aprile 2018, n. 21925.
[109] Cass. pen., Sez. II, 5 giugno 2015, n. 27806.
[110] Cass. pen., Sez. IV, 12 dicembre 2006, n. 4170.
[111] Accinni (2018), pp. 27 ss.
[112] Sturzo (2018), p. 29.

6. Riflessioni conclusive *de iure condendo*.

Alla luce degli evidenziati rischi penali generati da un fenomeno virtuale in continua evoluzione, si deduce che il nostro ordinamento sia già dotato di alcuni strumenti di contrasto al *cyberlaundering*, potendo fare ricorso alle fattispecie codicistiche in tema di riciclaggio senza che questo comporti forzature ermeneutiche o vietate applicazioni analogiche.

Pur tuttavia deve ravvisare la necessità di una maggiore regolamentazione in materia, auspicando un intervento legislativo teso alla repressione del riciclaggio digitale.

Oltre a intervenire con la previsione di una fattispecie *ad hoc*, si ritiene possibile anche l'introduzione di una circostanza aggravante speciale[113], sulla falsa riga di quanto fatto in tema di contrasto al terrorismo internazionale tramite la disposizione di cui all'art. 270-*quinquies* c.p., che espressamente riferisce all'utilizzo degli strumenti informatici o telematici.

Va comunque accennata la valenza, in tale settore, della disciplina preventiva[114] introdotta con la Quinta Direttiva 2018/843/UE, definita come la "prima regolamentazione organica" in tema di valute virtuali, volta a garantire il rafforzamento dei poteri delle *Financial Intelligence Units* (FIU), la promozione di una maggiore cooperazione tra le stesse, la piena accessibilità dei registri e la pubblicizzazione delle informazioni in essi contenuti ai fini di garantire una maggiore trasparenza fiscale ma, soprattutto, l'estensione degli obblighi di adeguata verifica della clientela in capo a tutti i prestatori di servizi che operano *on-line*, in particolare agli *exchagers* e ai *wallet providers*.

Bibliografia:

Alcini, Jacopo (2018): "Mondi paralleli, *bitcoin* e reati virtuali", in *La giustizia penale*, 2, pp. 438- 448.

Amato Massimo e Fantacci Luca (2016): *Per un pugno di* Bitcoin, (Milano, Università Bocconi editore).

Bocchini, Roberto (2017): "Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche", in *Dir. inf.*, 1, pp. 27 ss.

Bordot, Ludovica (2016): " Il *Cyber-riciclaggio* e i paradisi fiscali: le nuove dinamiche nel processo di *cyberlaundering*", reperibile in *www.dspace.unive.it*.

Bricchetti, Renato (2014), *Riciclaggio e autoriciclaggio,* in *Riv. it. dir. proc. pen.*, 2, 684 ss.

Brunelli, David (2015): "Autoriciclaggio e divieto di retroattività: brevi note a margine del dibattito sulla nuova incriminazione", in *www.dirittopenalecontemporaneo.it.*

Capaccioli, Stefano (2015), *Criptovalute e* Bitcoin*: un'analisi giuridica* (Milano, Giuffré)

Castaldo, Andrea (2013): "Riciclaggio e impiego di beni di provenienza delittuosa", in Pulitanò, Domenico (a cura di), *Diritto penale. Parte speciale, tutela del patrimonio* (Torino, Giappichelli).

Castaldo, Andrea e Naddeo Marco (2010), *Il denaro sporco. Prevenzione e repressione nella lotta al riciclaggio,* (Padova, Cedam)

Cavallini, Stefano e Troyer, Luca: "Apocalittici o integrati? Il nuovo reato di autoriciclaggio: ragionevoli sentieri ermeneutici all'ombra del «vicino ingombrante»", in *www.dirittopenalecontemporaneo.it.*

Cerqua, Luigi Domenico (2008): "Il delitto di riciclaggio nel sistema penale italiano, in Cappa, Ermanno e Morera, Umberto (a cura di), *Normativa antiriciclaggio e segnalazione di operazioni sospette* (Bologna, Il Mulino).

[113] Plantamura (2019), p. 888.
[114] Per una disamina completa si rimanda al successivo contributo della Dott.ssa Ingrao.

Ciraulo, Antonella (2016): "voce Autoriciclaggio", in *Dig. Disc. Pen.*, aggiornamento.

Cocco, G (2011): "Una introduzione ai reati contro il patrimonio e l'economia pubblica tra beni giuridici e tecniche di tutela", in *Studi in onore di Mario Romano* (Napoli, Jovene editore)

Cucuzza, Osvaldo (2007): *Segreto bancario, criminalità organizzata, riciclaggio, evasione fiscale in Italia* (Padova, Cedam).

D'agostino, Luca (2018): "Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D.lgs. 90/2017", in *Riv. dir. banc.*, dirittobancario.it., 5.

Dell'Osso, Alain Maria (2017): *Riciclaggio di proventi illeciti e sistema penale* (Torino, Giappichelli)

Di Vizio, Fabio (2018): "Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti", in *www.dirittopenalecontemporaneo.it*.

Fiandaca, Giovanni e Musco, Enzo (2015): *I delitti contro il patrimonio, Diritto penale. Parte speciale*, vol. II (Bologna, Zanichelli).

Flor, Roberto (2012): "Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di *Internet*", in www.dirittopenalecontemporaneo.it

Flor, Roberto (2019): "La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative, in Cadoppi Alberto, Canestrari Stefano, Manna Adelmo, Papa Michele (a cura di), *Trattato di diritto penale – Cybercrime* (Milano, Utet giuridica), pp. 142- 192.

Gambaro, Antonio (2012): "I beni", in Cicu Antonio, Messineo Francesco, Mengoni Luigi, *Trattato di diritto civile e commerciale*, (Milano, Giuffrè).

Gasparri, Giorgio (2015): "Timidi tentativi di messa a fuoco del *bitcoin*: miraggio monetario o soluzione tecnologica in cerca di un problema?", in *Dir. Inf.*, pp. 417- 430.

Gullo, Antonio (2015): "Autoriciclaggio, voce per Il libro dell'anno del diritto Treccani 2016", in *www.dirittopenalecontemporaneo.it.*

Gullo, Antonio (2017): "Il delitto di autoriciclaggio al banco di prova della prassi: i primi (rassicuranti) chiarimenti della Cassazione", in *Dir. pen. proc.*, 4, pp. 482- 489.

Gullo, Antonio (2018): " La responsabilità dell'ente e il sistema dei delitti di riciclaggio", in Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo e Papa, Michele, *Diritto penale dell'economia* (Utet giuridica, Torino)

Gullo, Antonio (2018): " Realizzazione plurisoggettiva dell'autoriciclaggio: la Cassazione opta per la differenziazione dei titoli di reato", in *www.dirittopenalecontemporaneo.it.*

La Rocca, Laura (2015): "La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali", in *Analisi giuridica dell'Economia*, 1, pp. 201- 222.

Leslie, Daniel Adeoyè (2014): *Legal Principles for combatting Cyberlaundering, Law, Governance and Technology Series* (Switzerland, Springer International Publishing).

Mancini, Marco (2015): "Valute virtuali e *bitcoin*", in *Analisi giuridica dell'economia*, 1, pp. 117- 138.

Manes, Vittorio (2004): "Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale", in *Riv. Trim. dir. Pen. econ.*, 2004, 75 ss.;

Manes, Vittorio (2006): "(voce) Riciclaggio e reimpiego dei proventi illeciti", in Cassese, Sabino (a cura di), *Dizionario di Diritto pubblico* (Milano, Giuffrè), pp. 5226- 5230.

Masciandaro, Donato (2012): "Reati e riciclaggio: profili di analisi economica", in Cappa, Ermanno e Cerqua, Luigi Domenico (a cura di), *Il riciclaggio del denaro. Il fenomeno, il reato, le norme di contrasto* (Milano, Giuffré).

Mazzacuva, Nicola (1991), Artt. 23 e 24. Commento alla legge 55/90, in *Leg. Pen.*, pp. 501 ss.

Mezzetti, Enrico (2013): "Reati contro il patrimonio", in Grosso, Carlo Federico, Padovani, Tullio, Pagliaro, Antonio *Trattato di diritto penale, Parte speciale* (Milano, Giuffré).

Paliero, Carlo Enrico (2012): "L'Agorà e il Palazzo. Quale legittimazione per il diritto penale?", in *Criminalia*, pp. 102 ss.

Passerelli, Nina (2016), "*Bitcoin* e antiriciclaggio", in *Gnosis, Rivista italiana di* intelligence, rinvenibile sul sito internet istituzionale del SISR www.sicurezzanazionale.gov.it.

Pecorella, Gaetano (1989):"Denaro (sostituzione di)", in *Dig. disc. pen.*, vol. III, pp. 366 ss.

Picotti, Lorenzo (2008): "La ratifica della Convenzione *Cybercrime* del Consiglio d'Europa. Profili di diritto penale sostanziale", in *Dir. pen. proc.*, pp. 770- 716.

Picotti, Lorenzo (2017): "Quale diritto penale nella dimensione globale del *cyberspace*?", in Wenin, Roberto e Fornasari, Gabriele (a cura di), *Diritto penale e modernità. Le nuove sfide tra terrorismo, sviluppo tecnologico e diritti fondamentali*, (Trento, Editoriale scientifica)

Picotti, Lorenzo (2019): "Diritto penale e tecnologie informatiche: una visione d'insieme", in Cadoppi Alberto, Canestrari Stefano, Manna Adelmo, Papa Michele (a cura di), *Trattato di diritto penale – Cybercrime* (Milano, UTET).

Plantamura, Vito (2019): "Il *cybericiclaggio*", in Cadoppi Alberto, Canestrari Stefano, Manna Adelmo, Papa Michele (a cura di), *Trattato di diritto penale – Cybercrime* (Milano, Utet giuridica), pp.859- 890.

Rapetto, Umberto (1999): "Il riciclaggio del terzo millennio", in *Gnosis, Rivista italiana di* intelligence, rinvenibile sul sito internet istituzionale del SISR www.sicurezzanazionale.gov.it.

Rapetto, Umberto (1999): "Il riciclaggio del terzo millennio", in *Gnosis, Rivista italiana di* intelligence, rinvenibile sul sito internet istituzionale del SISR www.sicurezzanazionale.gov.it.

Seminara, Sergio (2005): "I soggetti attivi del reato di riciclaggio tra diritto vigente e prospettive di riforma", in *Dir. pen. e processo*, pp. 236 ss.;

Seminara, Sergio (2016): "Spunti interpretativi sul delitto di autoriciclaggio", in *Dir. pen. proc.*, pp. 1631 ss.

Sgubbi, Filippo (2015): "Il nuovo delitto di «autoriciclaggio»: una fonte inesauribile di «effetti perversi» dell'azione legislativa", in *www.dirittopenalecontemporaneo.it*.

Simoncini, Simone (2015): "Il *Cyberlaundering*: la «nuova frontiera» del riciclaggio", in *Riv. trim. dir. pen. econ.*, 4, pp. 897- 915.

Soldi, Giovanni Maria (2011): "Riciclaggio (II aggiornamento)", in *Dig. Disc. Pen.*, disponibile all'indirizzo www.pluris-cedam.utetgiuridica.it

Stokes, Robert (2012): "*Virtual Money Laundering: the case of Bitcoin and the Linden Dollar*", in *Information & Communications Technology Law*, pp. 221-250.

Sturzo, Ludovica (2018): "*Bitcoin* e riciclaggio 2.0", in *www.dirittopenalecontemporaneo.it*.

Vardi, Noah (2015): "Criptovalute e dintorni: alcune considerazioni sulla natura giuridica del *Bitcoin*", in *Dir. inf.*, pp. 443- 456.

Zanchetti, Mario (1997), *Il riciclaggio di denaro proveniente da reato*, (Milano, Giuffré).

Zenovich, Zeno (1989): "voce Cosa", in *Dig. Priv. Sez. civ.*, IV (Torino, Utet giuridica), pp. 438 ss.

La tutela penale della privacy nel cyberspazio

La tutela penal de la privacidad en el ciberespacio

Criminal Law and the Protection of Privacy in Cyberspace

I limiti della tutela penale del trattamento illecito dei dati personali nel mondo digitale

Los límites de la tutela penal del tratamiento ilícito de datos personales en el mundo digital

Limits to Criminalization of Unlawful Data Processing in the Digital World

Salvatore Orlando
Dottore di ricerca in Diritto penale presso l'Università di Palermo
salvatore.orlando@unipa.it

Privacy, Dolo Privacy, Dolo Privacy, Intention

Abstracts

L'incessante scambio di dati ed informazioni nel mondo del web ha imposto una rivisitazione dei paradigmi classici del bene giuridico della *privacy*. Emblematico è, in tal senso, il reato di *trattamento illecito dei dati personali*, di cui all'art. 167 Codice *privacy* (D. Lgs. 196/2003), oggetto di numerosi interventi correttivi per adeguarlo alle moderne e mutevoli esigenze di tutela. L'indagine riflette dunque sulla recente riforma (D. Lgs. 101/2018) che sembra voler recuperare l'offensività del tipo delittuoso attraverso la formulazione di un reato di evento il cui disvalore è incentrato sul *nocumento all'interessato:* tuttavia, in modo apparentemente inconciliabile, viene mantenuto un *dolo specifico di danno*, che si sovrappone al risultato materiale conseguito dall'agente. Infine, si cerca di dimostrare come stia emergendo una nuova oggettività giuridica di carattere pubblicistico, ossia il *sistema di protezione dei dati personali*, la cui tutela è demandata agli artt. 167-*bis* e 167-*ter*.

El permanente intercambio de datos e informaciones en el mundo de la web ha impuesto una revisión de los paradigmas clásicos de la privacidad como bien jurídico. El delito de tratamiento ilícito de datos personales, establecido en el art. 167 del Código de la Privacidad (Decreto Legislativo 196/2003), es emblemático en este sentido, habiendo sido objeto de numerosas modificaciones para adaptarlo a las necesidades modernas y cambiantes de protección. El presente trabajo reflexiona sobre la reciente reforma legislativa (Decreto Legislativo 101/2018), la cual pareciera intentar recuperar la lesividad del tipo penal a través de la formulación de un delito de resultado cuya lesión se centra en el daño a la persona afectada. Sin embargo, de forma aparentemente irreconciliable, se mantiene un animo específico de daño, que se solapa con el resultado material conseguido por el agente. Por último, se intenta demostrar cómo está surgiendo una nueva objetividad jurídica de carácter publico, es decir, el sistema de protección de datos personales, cuya protección se reserva a los artículos 167-bis y 167-ter.

The constant exchange of data and information in the world of the web has imposed a reinterpretation of the classic paradigms related to the so-called *privacy* as a legal interest. The crime of unlawful processing of personal data, as per art. 167 of the Italian Privacy Code (Legislative Decree 196/2003), is emblematic in this sense, and has been emended by numerous corrective measures in order to adapt it to the modern and changing needs of legal protection. The analysis carried out here therefore reflects on the recent reform (Legislative Decree 101/2018) which tries to recover the offensiveness of the criminal type through the formulation of a result crime whose offence is focused on the *harm* to the person concerned: however, in an apparently irreconcilable way, *a*

specific intent of damage is maintained, which overlaps with the material result achieved by the agent. Finally, the paper tries to demonstrate how a new legal interest with a public nature is emerging, that is, the *system of protection of personal data*, the protection of which is entrusted to Articles 167-bis and 167-ter.

Sommario

1. Profili introduttivi.

Il mondo delle connessioni digitali è pervaso da un *fil rouge* che virtualmente unisce gli utenti del *web* in un incessante scambio di informazioni, veicolate attraverso piattaforme immateriali. È noto come, al fine di essere parte di una comunità digitale, sia necessario comunicare i *propri dati personali* i quali, secondo dinamiche che rispondono ad algoritmi non intelligibili ai più, creano il nostro profilo identificativo nel *web*: in questo momento, abbiamo rinunciato *consensualmente* alla nostra assoluta signoria ed al controllo sui nostri dati personali[1].

Infatti, in una società ad altissima – e ancora crescente – informatizzazione delle attività e dei servizi, è inevitabile per ciascuno di noi la necessità di lasciare una traccia della propria attività, delle abitudini, delle caratteristiche e delle preferenze personali. Chi raccoglie i dati ricevuti procede poi al loro trattamento con finalità, tra le altre, di c.d. *profilazione* nell'ambito di attività di *marketing* o di classificazione dei cittadini che, in ultima istanza, possono prestarsi ad usi discriminatori o per scopi elettorali.

Ed in questo senso, sorgono evidenti questioni di tutela della c.d. *privacy* o più propriamente riservatezza. Sul tema la letteratura è sterminata: si parla talora di *privacy*, talaltra di *privatezza*, ovvero di *vita privata*, o ancora di *riservatezza*, alludendo a concetti non sempre coincidenti[2]. In particolare, la nozione di *privacy* – come "*diritto dell'età d'oro della borghesia*"[3] – fa il primo ingresso in Italia soltanto nel 1970 attraverso l'art. 8 dello Statuto dei lavoratori[4] che vieta la raccolta delle opinioni politiche, sindacali, religiose dei dipendenti.

Tuttavia, nel corso degli ultimi decenni il bene oggetto di tutela penale, dapprima dotato di una forte connotazione individualistica, è andato assumendo via via una natura pubblicistica, appuntandosi ormai, come meglio si vedrà, sul piano della *protezione dei dati personali*[5].

In questo breve contributo si intende, da un lato, illustrare criticamente i profili giuridici più significativi e i limiti della tutela penale che il legislatore ha dovuto affrontare – con risultati certo altalenanti – nella formulazione di tipi delittuosi diretti alla tutela del bene della *privacy;* dall'altro lato, segnalare le aporie del sistema di tutela apprestato e, dunque, vagliare attentamente le soluzioni ermeneutiche offerte dalle Corti, che – seppur in sporadiche decisioni – hanno ricostruito la *ratio legis* di protezione di un bene giuridico tanto di recente emersione, quanto di notevole rilevanza nel contesto contemporaneo e prevedibilmente ancora crescente in futuro.

In questo senso, constatata dapprima l'evoluzione concettuale della *privacy* ed evidenziati i possibili profili di interesse penalistico – seppur, si avverte, soltanto marginali all'interno del *mare magnum* degli aspetti riconducibili al tema – ci si concentra sui problemi di tecnica legislativa. In relazione infatti ad una tutela che trova incontestabile legittimità sul versante costituzionale, numerose questioni sorgono al momento di individuarne tanto i limiti quanto gli strumenti di attuazione, nella correlata prospettiva del rispetto dei principi di materialità, determinatezza ed offensività, nonché della effettività della risposta giuridica. La complessità della materia è testimoniata dal '*travaglio legislativo*' che ha segnato il nostro ordinamento in tema di tutela della *privacy,* il quale trova esemplificazione nelle notevoli modifiche appor-

[1] In relazione ai notevoli rischi (non solo incidenti sull'interesse penalmente rilevante della *privacy*) dei c.d. *Social Network*, ossia delle piattaforme web di condivisione di dati, informazioni e notizie personali, si veda, Picotti (2012), p. 2522; altresì, Galdieri (2012), p. 2697.
[2] Bricola (1967), 1114.
[3] Così, Rodotà (2005), 12.
[4] L. 20 maggio 1970, n. 300 "*Norme sulla tutela e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento*".
[5] In ambito penalistico, il riferimento alla riservatezza come bene degno di tutela viene introdotto con la Legge 8 aprile 1974, n. 98 "*Tutela della riservatezza e della libertà e segretezza delle comunicazioni*", che introduce alcune fattispecie delittuose tra le quali, l'art. 615-bis *Interferenze illecite nella vita privata,* inserito nel capo III, sez. IV (Delitti contro la inviolabilità del domicilio) titolo XII (Delitti contro la persona), l'art. 617-bis *Installazione di apparecchiature atte a intercettare o impedire comunicazioni telegrafiche o* telefoniche, e l'art. 617-ter *Falsificazione, alterazione o soppressione di contenuto di comunicazioni o conversazioni telegrafiche o telefoniche.*

tate alla fattispecie di *trattamento illecito dei dati personali*, di cui all'art. 167 del Codice della *privacy*[6]. Come meglio si cercherà di dimostrare nel corso dell'indagine, la norma è costruita secondo una progressione criminosa attenta a selezionare le condotte meritevoli di punizione attraverso il dolo specifico e, con l'ultima modifica intervenuta con il D. Lgs. 101/2018, configura un reato di evento il cui disvalore appare incentrato sulla lesione ad un bene individuale, mediante il ricorso all'espressione del "*nocumento all'interessato*". Pur tuttavia, a seguito della riforma, il fuoco dell'incriminazione si sposta verso una nuova oggettività giuridica (meglio, un bene-categoria) di carattere pubblicistico, ossia il *sistema di protezione dei dati personali*, la cui tutela è demandata ora agli articoli 167-*bis* e 167-*ter*.

2. La *Privacy*: possibili profili penalistici in un mondo digitale.

Orbene, in primo luogo, appare possibile – nonché opportuno – distinguere i concetti di *privacy* o riservatezza[7] e quello di diritto alla protezione dei dati personali, i quali indicherebbero oggettività giuridiche tra loro in parte differenti: è, infatti, preliminare vagliare il significato dell'interesse che si intende salvaguardare nonché gli scopi di tutela perseguiti attraverso lo strumento penale[8].

Il concetto di *privacy* viene elaborato per la prima volta nell'Ottocento nel mondo anglosassone – in cui storicamente più alto è stato il "*grado di sensibilizzazione*" in materia[9] – da parte di due giuristi, Warren e Brandeis[10], che ne hanno individuato il nucleo costitutivo nel celeberrimo *right to be let alone*, il diritto di essere lasciato da solo. In questo senso, in una accezione ancora primordiale ma mai veramente superata, si tentava di porre l'accento su quell'innata esigenza dell'uomo di escludere gli altri dalla conoscenza di sé stessi e della propria sfera personale. È alquanto curioso come – seppur in un contesto non ancora globalizzato e affatto digitalizzato – questa esigenza si manifestasse in aspetti solo in parte differenti da quelli che oggi rilevano, come ad esempio, nella segretezza della corrispondenza o nella non diffusione di fotografie a mezzo stampa. Questa esigenza dunque – che potenzialmente può rivolgersi tanto ai poteri pubblici quanto alle interferenze private – si è andata evolvendo, lasciando tuttavia in eredità problemi definitori in ordine alla individuazione di una nozione univoca di *privacy*. Così, si è andato delineando un '*catalogo aperto*' che riguardasse, in generale, la tutela della sfera privata dell'individuo: la necessità di limitare l'accesso di altri alla propria sfera personale; il diritto di tenere determinate questioni segrete agli altri; la tutela della propria personalità, identità e dignità; il diritto all'intimità, ossia al riserbo circa le proprie relazioni personali o determinati aspetti della propria vita[11].

Della *privacy* quale oggetto di tutela si è soliti individuare un duplice contenuto[12]: un nucleo originario e tradizionale, afferente per l'appunto al c.d. *right to be let alone*, dal quale discende il diritto alla conoscenza esclusiva delle vicende relative alla propria vita privata (ovvero, da altra prospettiva, all'assenza di informazioni su noi stessi da parte degli altri); e un interesse al controllo esterno dei propri dati personali, in funzione di una corretta utilizzazione degli stessi[13].

In quest'ultimo senso, dunque è possibile già scorgere una *dimensione sociale della privacy* che si aggiunge al tradizionale aspetto individualistico della medesima e che riguarderebbe il problema del corretto e trasparente trattamento dei dati personali, che può manifestarsi in una duplice direzione: da un lato, si profilerebbe con un contenuto c.d. negativo (si suole dire,

[6] Ossia, il D. Lgs. 30 giugno 2003, n. 196, il quale, a seguito dell'ultima riforma intervenuta con il D. Lgs. 101/2018 (cfr. *infra* par. 4), è intitolato "*Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*".

[7] Nel senso di una totale coincidenza dei due concetti, Pizzetti (2016), p. 45. Sul rapporto tra *privacy* e diritto alla riservatezza, da ultimo si v. Manna, Di Florio (2019), p. 892.

[8] Sul punto, il quesito era stato posto, già a seguito della prima riforma in materia, su cui *infra* par. 3., da Sgubbi, (1998), p. 75.

[9] Cosi, Bricola (1967), p. 1081.

[10] Warren e Brandeis (1890), p. 193.

[11] In questi termini, si veda, Lamanuzzi (2017), p. 221.

[12] Patrono (1986), p. 557 s.

[13] Sui profili problematici tra diritto alla riservatezza e libertà di informazione, e dunque di divulgazione di notizie afferenti alla vita privata, si veda, tra gli altri, Vigevani (2016), p. 473. Non v'è dubbio, peraltro, che nel mondo digitale la dualità si pone in termini differenti, in quanto il *web* si configura come uno spazio di deresponsabilizzazione e, per certi versi, come un *freies Raumrecht*.

libertà da), che ricomprenderebbe il diritto a mantenere il riserbo su certi dati, o comunque a limitarne la circolazione latamente intesa (il che atterrebbe ancora alla riservatezza *strictu sensu*); dall'altro lato, avrebbe, invece, un contenuto positivo (si suole dire, *libertà di*), che assumerebbe una valenza poliedrica, dovendo essere garantiti alla *platea di interessati* (si noti, fin d'ora, l'ampiezza dei titolari) i mezzi (ad es., l'accesso e la cancellazione) necessari alla correttezza del trattamento degli stessi, al fine di salvaguardare, in primo luogo, l'identità personale di coloro ai quali i dati si riferiscono[14].

In questo variegato contesto, si staglia nella *materia penalistica* il lavoro di Franco Bricola[15], il quale oltre mezzo secolo fa parlava della riservatezza e della sua rilevanza sociale già in termini preoccupati, riservando la sua trattazione alle possibili interferenze nella vita privata, con specifico riguardo ai profili di interesse pubblico alla non diffusione delle informazioni personali.

In questo senso – avendo definito la stampa e la televisione mezzi idonei all'espropriazione *per pubblica curiosità* – distingueva tre sfere più particolari della vita privata, in contrapposizione all'interesse alla *vita di relazione*, in cui rientrerebbe la tutela della reputazione[16]: la sfera privata *strictu sensu* (*Privatsphäre*) che ricomprende tutti quei comportamenti, notizie o informazioni che il soggetto *desidera* non divengano di pubblico dominio; la sfera confidenziale (*Vertrauensphäre*) che ricomprende quegli avvenimenti, discorsi o notizie di cui il soggetto rende partecipi persone di particolare fiducia; e infine, la sfera del segreto (*Geheimsphäre*) che ricomprende tutte quelle notizie e fatti che per interessi o ragioni particolari sono inaccessibili a chiunque non sia titolare del segreto (e ne abbiano dunque ricevuto il consenso). Le tre sfere possono immaginarsi come tre cerchi concentrici di raggio progressivamente minore e ad esse la dottrina ha fatto riferimento, quando ha affrontato il tema del diritto alla riservatezza.

In questo contesto, merito del lavoro di Bricola è quello di iniziare a distinguere due momenti in cui sussisterebbe un bisogno di tutela penale: il momento delle *interferenze esterne* nella sfera privata che è presidiato dal diritto al rispetto alla vita privata, nel senso dunque più pregnante; ed il momento della *diffusione* e *divulgazione* di notizie e informazioni, ancorché legittimamente acquisite, la cui difesa spetterebbe, invece, al diritto alla riservatezza. E, con riferimento a quest'ultimo, si spinge ad un ulteriore *discrimen*, che sembra anticipare ed ispirare le scelte incriminatrici più recenti: egli distingue, da un lato, tra la violazione del segreto che sussisterebbe nel caso di conoscenza illegittima (dunque, senza consenso) di dati confidenziali racchiusi, ad esempio, nella corrispondenza e, dall'altro, la violazione del diritto alla riservatezza che si ha nel caso di rivelazione a terzi della notizia da parte del soggetto destinatario della fiducia.

La demarcazione è sottile, ma estremamente utile ai fini del corretto inquadramento dell'attuale sistema di tutela della *privacy*, nella sua declinazione di *protezione dei dati personali*, che si insinuerebbe in questo reticolo concettuale, per l'appunto, tra la tutela del segreto della vita privata[17], quest'ultimo inteso nel senso più ampio, e la tutela della riservatezza, ossia nell'interesse alla *non diffusione* di informazioni relative alla propria sfera privata[18]. Ed è dunque tenendo conto di questa ambivalenza che deve essere intesa l'evoluzione recente della legislazione in materia di *privacy*[19].

In questo senso, si è mossa anche la costruzione di una tutela penale che – in una prospettiva sostanzialistica – ha tentato di dare rilievo ad un valore – quello della riservatezza – avente originariamente un forte *margine di relatività*, in relazione alla diversa sensibilità ed esigenze che può legittimamente avere il titolare, ma che, a ben vedere, atteso un nucleo essenziale "*costante per la media dei cittadini*", si pone tra la rilevanza scriminante del consenso e l'interesse

[14] Si veda, Veneziani (2001), p. 369.
[15] Bricola (1967), p. 1114 ss.; illuminanti altresì i contributi di Mantovani (1968), p. 61 ss.; Palazzo (1975), p. 126 ss.
[16] L'interesse alla reputazione è tutelato dall'art. 594 c.p. che punisce il reato diffamazione. A ben vedere, l'interesse alla vita di relazione e l'interesse alla vita privata possono sussistere nello stesso caso concreto ed in tal senso possono sorgere problemi di concorso di reati, sul punto cfr. Carnelutti (1955), p. 5 s.
[17] A tal proposito, ma si tornerà anche in seguito, cfr. Cass. Pen., Sez. VI, 21.02.2013, n. 9726, in relazione alla rivelazione ed utilizzazione di segreti di ufficio.
[18] Sul punto, si può vedere altresì il recente lavoro di D'Agostino (2019), in part. 5 ss.
[19] Negli ultimi anni la nozione di *privacy* è stata invocata in una accezione funzionale che tende a distanziarla da quella di riservatezza e ad identificarla con il diritto protezione dei dati personali. La sovrapposizione che si registra – tra *privacy* e protezione dei dati personali – è dovuta principalmente al fatto che la legge organica che contiene la sua disciplina va sotto il nome di codice della privacy e l'autorità preposta alla sua corretta implementazione Garante della *privacy*. Quindi, convenzionalmente, viene il termine privacy nel senso di protezione dei dati personali, il quale sottende ovviamente anche un interesse generale a che la circolazione dei dati avvenga in modo lecito e trasparente senza finalità ulteriori di propaganda politica o di marketing, cfr. Pizzetti (2016), 45.

pubblico alla divulgazione delle notizie.

Così, in un percorso storico-penalistico, in cui i concetti di valore come la reputazione ed il decoro[20] hanno cominciato a segnare una rinuncia allo strumento penale[21], la tutela della *privacy* – seppur strettamente legata a questi ultimi[22] – ha, invece, mutato i propri fini e le tecniche di incriminazione[23].

3. La tutela della *privacy* all'insegna di un diritto penale emergenziale

Ad una valutazione d'insieme, l'osservatore della materia non può non accorgersi che il sistema penale di tutela della *privacy* appare caratterizzato, fin dalle sue embrionali formulazioni, dal ricorso, in via emergenziale e rapsodica, a strumenti sanzionatori nuovi e a costruzioni di tipi delittuosi censurabili di incostituzionalità.

In un panorama in cui si stagliano sullo sfondo le sfide delle nuove e problematiche frontiere tecnologiche[24], il diritto penale ha reagito per lo più in modo disarmonico e disorganico fino ad assumere il volto di una *legislazione emergenziale*. Ciò si evince dal tentativo del legislatore di reprimere *tout court* le condotte indesiderabili, anticipando le soglie di punibilità o formulando fattispecie di pericolo[25].

Come noto, la natura frammentaria del diritto penale è frutto di una società tradizionale e di schemi di comportamento familiari alla coscienza sociale. Il legislatore, invero, tanto nell'ottica dell'armonizzazione comunitaria imposta dalla Direttiva 95/46/CE[26], quanto nella prospettiva di massima repressione dei nuovi fenomeni emersi nel mondo del digitale che avevano suscitato grande allarme sociale, ha, invece, tentato di abbracciare tutte le ipotesi possibili, formulando tipi delittuosi connotati da indeterminatezza e genericità, anticipando la punibilità a ipotesi di mera messa in pericolo del bene tutelato.

Un fenomeno collegato a tale constatazione è quello dell'emersione di una *nuova funzione al giudice penale*, il quale – si può dire, *obtorto collo* – crea diritto: nel caso della tutela della *privacy*, lo si vedrà meglio con riguardo al trattamento illecito dei dati personali, il legislatore affida al giudice l'individuazione dell'ambito realmente appropriato di applicazione della legge. In questo senso, il diritto penale, facendo ricorso ad una legislazione simbolica, demanda alla prassi giudiziaria – ossia al "diritto vivente" – l'onere di provvedere alla sua efficienza[27].

Ciò premesso, al fine porre rimedio a costruzioni legislative esposte a rischi tanto di inefficacia quanto di incostituzionalità, è preliminare affrontare la questione circa la possibile individuazione di un bene-categoria[28], al quale riferire l'offesa in maniera sostanzialmente uniforme dal punto di vista del tipo di interesse tutelato: nella materia *de qua* appare oggi pacifico che la rilevanza costituzionale dell'interesse della riservatezza sembra essere ancorato all'art.

[20] Sui possibili collegamenti tra disciplina della *privacy* e reputazione, si veda, Seminara (1998), p. 911. Inoltre, mai superate le riflessioni di Musco (1974), in part. p. 133 s.

[21] Si pensi, a titolo esemplificativo, alla parziale depenalizzazione in materia di atti osceni, di cui all'art. 527 c.p. che oggi prevede una sola sanzione pecuniaria amministrativa, a seguito dell'introduzione del D. Lgs. 8/2016; si pensi, altresì, al reato di ingiuria che è stato depenalizzato con il D. Lgs. 7/2016.

[22] Sul punto, si veda Manna (1998), p. 260.

[23] Scrive Fiore (1999), p. 1 che "[…] *nel mondo contemporaneo, la riservatezza, quale espressione tanto del diritto della personalità quanto del bene dell'onore, ha svolto il ruolo di una sorta di estremo baluardo eretto per l'appunto contro l'erosione del valore dell'individualità in una società fortemente orientata all'omologazione dei comportamenti sociali e degli atteggiamenti culturali e quindi ad alto rischio di discriminazione*".

[24] Cfr. per una panoramica generale sui nuovi "rischi" della tecnologia e dell'informatica, si v., per tutti, Militello e Spena (2018).

[25] Cfr. Grasso (1986), p. 689 ss.; Marinucci (1987), p. 19 s.; Pulitanò (1987), p. 33 s.; Canestrari (1991), p. 7 ss.; Angioni (1994); M. Romano (1995), p. 319 s.; Parodi Giusino (1999), p. 687 ss. Altresì sul punto, sono interessanti le riflessioni in materia ambientale, che, per quanto concerne la tutela penale apprestata, appare per certi versi affine alla materia che è oggetto della presente indagine, cfr. Giunta (1997), p. 1102.

[26] Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 "*relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati*".

[27] Ad esempio, Troncone (2014), p. 2066, secondo cui il reato sul trattamento illecito dei dati personali sarebbe "*una norma laboratorio*", da cui discendono "*le problematiche dei più significativi nodi teorici del diritto penale ma anche il legislatore non ha munito di quei dispositivi per risolvere le ipotesi applicative controverse*".

[28] Nonostante – fuori da una legislazione penale organica non dotata di funzioni sistematiche – sia difficile che la *ratio legis* di ogni singola norma possa contribuire a comporre uno scopo di tutela unitario: in questo senso, si vedano le osservazioni di Pagliaro (1965), p. 389 s., che propende per una "nozione metodologica del bene tutelato" che, valorizzando la *ratio* di ogni singola norma incriminatrice, si discosta dalla della possibilità di individuazione di un oggetto giuridico di categoria.

2 della Costituzione, la cui natura di 'clausola aperta' ne consente il pieno riconoscimento[29], ed altresì all'art. 7 della Carta di Nizza[30] ed all'art. 8 della Convenzione Europea dei diritti dell'uomo[31], norme che come è noto trovano ingresso nel nostro ordinamento rispettivamente attraverso gli artt. 11 e 117 Cost.

Orbene, acquisito questo dato – certamente necessario, ma non ancora sufficiente per ancorare una protezione penalistica – si pone il quesito principale sui limiti della tutela da apprestare al bene giuridico della *privacy*, nella sua declinazione, come visto, della *protezione dei dati personali*. In altri termini, assodata la legittimità sul versante costituzionale della tutela penale della riservatezza, il problema si sposta – e per vero, come sempre, diviene delicato – nel momento nel quale da quest'assunzione di carattere generale e generico si deve passare alla concreta definizione degli strumenti di tutela, che possono legittimare l'intervento repressivo nell'ottica del rispetto dei principi di sussidiarietà, determinatezza e offensività[32].

In un contesto in cui si è passati da una tendenza all'espansione dell'intervento penale[33], soprattutto in campi emergenti come quelli dell'economia e del mondo digitale, si è da ultimo giunti ad una prospettiva legislativa di depenalizzazione e dunque di arretramento dell'area del penalmente rilevante.

Ed in questo senso, soprattutto in epoche di grandi tensioni sociali o di emergenze repressive, l'obiettiva difficoltà di determinare i caratteri essenziali degli oggetti di tutela e dunque individuare le condotte idonee ad offenderli ha indotto il legislatore – con la prima forma di incriminazione del trattamento illecito dei dati personali di cui alla L. 675/1996[34] – a percorrere la strada di una forte anticipazione della soglia di punibilità a momenti di *pericolo astratto* o *presunto*, in cui il verificarsi di un danno effettivo – e dunque di un'offesa ad un bene individuale – non era elemento essenziale per l'integrazione della fattispecie e dunque presupposto per la punibilità, ma era tipizzato quale circostanza aggravante, secondo la costruzione di un reato aggravato dall'evento[35].

Con la novella del 1996 – che avrebbe poi rappresentato il modello base su cui il legislatore è intervenuto a più riprese – si puniva "*chiunque, al fine di trarre per sé o per altri profitto o di arrecare ad altri un danno, procede al trattamento di dati personali in violazione degli artt. 11, 20 e 27, è punito con la reclusione sino a 2 anni o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da tre mesi a due anni*" (art. 35).

Con una infelice formulazione legislativa, dunque veniva introdotto un mero delitto di infedeltà o di inottemperanza[36] il cui disvalore era tutto incentrato sulla violazione degli artt. 11, 20 e 27 della stessa legge[37]: in questo senso non veniva costruita una fattispecie incriminatrice dotata di un contenuto materiale afferrabile e la cui modalità di aggressione al bene-categoria individuato non sembrava poggiare su solide basi, in quanto la fattispecie – si lamentava – era strutturata come *clausola sanzionatoria dei precetti extrapenali*[38].

[29] Per tutti, Bricola (1967), p. 1114; più di recente altresì Troncone (2011), p. 23 s. In giurisprudenza, cfr. Cass. sez. III, 9 giugno 1998, n. 5658, che definisce la riservatezza un «*diritto soggettivo perfetto*», che protegge «*situazioni e vicende strettamente personali, ancorché verificatesi fuori dal domicilio domestico, da ingerenze che, sia pure compiute con mezzi leciti e senza arrecare danno all'onore, al decoro o alla reputazione, non siano tuttavia giustificate da un interesse pubblico preminente*» e ricava la tutela costituzionale della vita privata di un soggetto dal complesso dei principi della Carta e dunque, oltre che dall'art. 2, anche dall'art. 3 e dagli artt. 14, 15, 27, 29 e 41 Cost.

[30] Art. 7 Rispetto della vita privata e della vita familiare: "*Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni*".

[31] Art. 8 *"1. Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui*

[32] Così, altresì Mucciarelli (2004), p. 173; cfr. Fiore (1999).

[33] Parla di "panpenalismo", invece, Manna (1993), p. 179 s.

[34] La legge n. 675 del 1996 ha rappresentato il primo sostanziale intervento direttamente finalizzato a regolamentare in maniera organica il diritto alla riservatezza e le modalità della sua tutela. La legge, anche per dare attuazione a sollecitazioni provenienti da fonti europee (in particolare la direttiva 95/46/CE *Tutela delle persone fisiche con riferimento al trattamento dei dati personali e alla loro libertà di circolazione*) esordiva con la solenne affermazione secondo cui il trattamento dei dati personali si svolge "*nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale* " (art. 1) ponendo un decisivo punto fermo nella lunga diatriba in ordine alla dimensione costituzionale della riservatezza, in quanto diritto assoluto e fondamentale dell'individuo.

[35] Sulla rilevanza del *nocumento* quale circostanza aggravante del reato, si veda Corrias Lucente (1997), p. 82.

[36] Manna (2001), p. 346.

[37] Ai sensi della L. 675/1996, prima della riforma intervenuta nel 2003, l'art. 11 riguarda il problema del consenso al trattamento. L'art. 12 pone però subito alcune eccezioni alla necessità del consenso e ciò significa come il consenso stesso non sia, in realtà, requisito indefettibile della fattispecie. L'art. 20 concerne i requisiti per la comunicazione e diffusione dei dati, mentre l'art. 27 ha per oggetto il trattamento da parte dei soggetti pubblici.

[38] Veneziani (2001), p. 376.

Peraltro, la disposizione incriminatrice citata si inseriva in un contesto normativo connotato da "*grande oscurità*"[39], in cui era massiccio il ricorso al modello delittuoso a discapito di quello contravvenzionale[40]. Da qui, sono affiorate in dottrina molte perplessità circa l'ancoraggio della fattispecie incriminatrice del trattamento illecito – unitamente alle altre figure di reato introdotte dalla L. 675/1996[41] – alla tutela della *riservatezza*, la cui effettiva lesione non rilevava ai fini della punibilità, ma residuava solo nell'espressione dell'eventuale nocumento, ma ai soli fini dell'aggravamento della pena. D'altronde, la legge citata ha rappresentato uno spartiacque nell'evoluzione concettuale della riservatezza, che – affrancandosi dalla concezione tradizionale risalente agli studi di Bricola – si affacciava al mondo del digitale, assumendo una terminologia differente, per l'appunto *privacy*, con un'accezione funzionale[42] nel senso della protezione dei dati personali, onde specificarne la natura di tutela di *interessi generali* alla non diffusione di informazioni personali ed alla *salvaguardia di mere funzioni*, e segnatamente delle funzioni di controllo e di intervento del Garante per la protezione dei dati[43].

Dunque, le scelte legislative *generaliste* e *panpenalizzanti*[44] in materia venivano state in parte ridimensionate con l'introduzione nel 2003 del c.d. *Codice della Privacy* (ma, in realtà, intitolato "*Codice in materia di protezione dei dati personali*"[45]), che cristallizzava definitivamente il superamento del bene-categoria individuale della riservatezza a favore di una nuova oggettività giuridica, e che fu "*ispirato all'introduzione di nuove garanzie per i cittadini, alla razionalizzazione delle norme esistenti e alla semplificazione*"[46].

Con riferimento alla fattispecie di trattamento illecito dei dati personali, il legislatore del 2003 segnava il passaggio ad un delitto caratterizzato dalla condizione obiettiva di punibilità[47], in cui la punibilità era subordinata alla derivazione dal fatto di un *nocumento*[48]. In questo modo, pur mantenendo il precetto penale del tutto incentrato sulla violazione delle disposizioni di natura extrapenale previste all'interno del nuovo Codice della *Privacy*, la loro mera *disobbedienza* non determinava *per se* l'integrazione del reato, se non fosse stata accompagnata dalla derivazione di un nocumento, considerato in senso lato[49].

Il requisito del *nocumento* assumeva dunque i requisiti di elemento del fatto di reato (e non più mera circostanza aggravante), entrando nella fattispecie tipica[50] quale condizione obiettiva di punibilità c.d. intrinseca[51]. Secondo tale impostazione, l'elemento del nocumento non

[39] Manna (2001), p. 344.
[40] Cfr. sul ruolo degli interessi tutelati per la scelta della natura delle sanzioni, cfr. Padovani (1984), p. 465; Id. (1987), p. 670.
[41] Si fa riferimento all'art. 34 "*omessa o infedele notificazione*", l'art. 36 "*omessa adozione di misure necessarie alla sicurezza dei dati*", in cui si rinviava ad una fonte extrapenale, che sollevava censure per violazione del principio di riserva di legge; e, infine, l'art. 37 "*inosservanza dei provvedimenti del Garante*".
[42] Pizzetti (2016), p. 45.
[43] Veneziani (2001), p. 377, il quale si chiedeva dell'opportunità del ricorso all'illecito penale piuttosto che a quello amministrativo, che appariva più adeguato.
[44] Altresì, Veneziani (2001), p. 372.
[45] D. Lgs. 30 giugno 2003, n. 196.
[46] Il codice mantiene pesanti sanzioni pecuniarie aventi natura amministrativa nelle ipotesi di omessa o inidonea informativa all'interessato (art. 161), omessa o incompleta notificazione (art. 163) e di omessa informazione o esibizione al Garante (art. 164), devolvendo l'applicazione delle stesse sanzioni al Garante, quale organo principe del sistema posto a presidio della riservatezza.
[47] Cfr. *infra*. In dottrina, si veda, tra gli altri Musotto (1936); Pagliaro (1960); Giuliani (1966); Angioni (1989), p. 1140 s.; M. Romano (1992), p. 39 s.; D'Ascola (1993), p. 652 s.; Insolera e Stortoni (2001), p. 413 s.; Bricola (2007), pp. 588 s.; nella manualistica, Pagliaro (2003), p. 393; Antolisei (2003), p. 697; Fiandaca e Musco (2012), p. 813; Mantovani (2017), p. 782.
[48] Cfr. Cass. Pen., Sez. V, 28.09.2011, n. 44940 secondo cui "*Sussiste continuità normativa tra il previgente reato di cui all'art. 35 della L. 675/1996 e la nuova fattispecie incriminatrice introdotta dall'art. 167 D. Lgs. 196 del 2003; né rileva in senso contrario che il nocumento alla persona offesa – previsto da entrambe le fattispecie di reato – costituisca nel reato previgente di pericolo presunto una circostanza aggravante, e condizione obiettiva di punibilità in quello vigente, in quanto quel che rileva è che il fatto (condotta ed elemento psicologico) costituente reato nella normativa previgente lo sia anche in quella vigente*", ed ha precisato che la legge previgente deve ritenersi più favorevole all'imputato, potendo la circostanza aggravante – a differenza della condizione obiettiva di punibilità – costituire oggetto del giudizio di bilanciamento, ex art. 69 c.p. *Conf.* Cass. Pen., Sez. III, 26 marzo 2004, n. 28680.
[49] Non vi era un esplicito ancoraggio del nocumento agli interessi o diritti di un soggetto persona fisica (ossia, ad es., *nocumento all'interessato* ovvero *nocumento agli interessi dell'interessato*), tanto che sarebbe stato plausibile ritenere il concetto di nocumento potenzialmente di portata più ampia rispetto ad una offesa individuale, cfr. Art. 167 Codice della Privacy: "*[1] Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi. [2] Salvo he il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni*".
[50] In questo senso, Pagliaro (1960); Id. (2003), p. 394. *Contra* Antolisei (2003), p. 697; altresì Mantovani (2017), p. 782, secondo i quali le condizioni obiettive di punibilità non entrerebbero a far parte della tipicità della fattispecie.
[51] Esempi di condizione obiettiva di punibilità si rinvengono nell'Art. 423 cpv., Art. 580 c.p., Art. 640 c.p.; in dottrina, con riguardo al piano degli interessi tutelati, si è distinta una condizione obiettiva di punibilità c.d. intrinseca (accadimento lesivo del bene protetto) da

avrebbe dovuto rappresentare oggetto del dolo, così da non restringere oltremodo l'area del penalmente rilevante, seppur fosse necessario, non essendo elemento estraneo (ma, appunto, intrinseco) al piano dell'offesa – nel rispetto del principio di colpevolezza come scolpito dagli insegnamenti della Corte Costituzionale[52] – quel *minimum* psicologico ravvisabile nella prevedibilità del fatto offensivo per l'imputabilità del reato a titolo di colpa[53].

In effetti, sarebbe stato *incongruo* prevedere quale evento del reato – e dunque oggetto del dolo – proprio la concretizzazione del fine di danno perseguito dal soggetto, che, in quanto riconducibile ai caratteri del dolo specifico, non è necessario che si realizzi ai fini della consumazione del reato[54].

Nel senso di una condizione obiettiva di punibilità intrinseca deponeva poi la stessa *ratio* della fattispecie che, onde prevenire la punizione di fatti non concretamente lesivi del bene individuale della *privacy*, richiederebbe che dalla condotta – già di per sé illecita perché in violazione del precetto extrapenale richiamato *per relationem* – sia derivata un'offesa dell'interesse protetto "*che è già potenzialmente realizzata dal fatto in senso stretto*"[55].

Orbene, come ha riconosciuto la stessa Corte di Cassazione[56] "*la modifica più evidente apportata dal d.lgs. n. 196/2003 all'art. 35 l. n. 675/96 (ora art. 167) consiste sul piano strutturale nella previsione nella fattispecie-base dell'elemento del "nocumento", attraverso la locuzione "se dal fatto deriva nocumento", precedentemente costituente soltanto una circostanza aggravante*», con la conseguenza che il delitto di illecito trattamento di dati veniva trasformato da reato di pericolo astratto o presunto a quello di pericolo concreto o 'effettivo', per il necessario accertamento della lesione al bene tutelato[57].

La riforma legislativa è sintomatica del cambio di prospettiva del legislatore delegato che ha tentato di riaffermare l'offensività del tipo delittuoso e di agganciare le modalità di aggressione ad una condotta materiale dotata di un concreto disvalore penale, lesiva del bene individuale della *privacy* (a discapito di un bene poco afferrabile come quello della salvaguardia di

una c.d. estrinseca (accadimento da cui dipende solo l'opportunità di punire), cfr. Nuvolone, *Il diritto penale del fallimento e delle altre procedure concorsuali*, Milano, 1955, 14; Pagliaro (2003), p. 395, secondo cui le condizioni intrinseche sono "*veri e propri eventi mascherati*"; Bricola (2007), pp. 588. Per precisazioni critiche, cfr. Angioni (1989), pp. 1440; inoltre, Brunelli (2013), p. 80, sostiene che le condizioni intrinseche, in quanto elementi marginali, ma non estranei al fatto tipico, devono essere imputabili per colpa come "coefficiente soggettivo vicario conforme al principio di colpevolezza". Egli, peraltro, conclude censurando di infondatezza la distinzione tra condizioni obiettive di punibilità intrinseche ed estrinseche in quanto deve sostenersi la natura giuridica di evento del fatto di reato "giacché solo in tal modo non si tradisce la vera portata del canone costituzionale indotto dal principio di colpevolezza" (83). Si veda, infine, il Progetto Pagliaro (art. 13) che escludeva le condizioni obiettive intrinseche, atteso che veniva prescritto che le condizioni obiettive di punibilità dovessero essere estranee al piano dell'offesa tipica.

[52] Cfr. Corte Costituzionale n. 364/1988, con nota di Pulitanò (1988), p. 686.

[53] *Funditus* Angioni (1989), pp. 1440 s., secondo cui il principio di colpevolezza potrà considerarsi rispettato solo se le condizioni di punibilità siano coperte perlomeno dalla colpa in senso stretto; cfr. altresì Fiandaca e Musco (2012), p. 819; peraltro si erano espresse diffuse perplessità circa la legittimità costituzionale delle condizioni obiettive di punibilità c.d. intrinseche per violazione del principio di colpevolezza, cfr. Dolcini (2000), pp. 863, per il quale "soltanto gli elementi estranei alla materia del divieto (come le condizioni estrinseche di punibilità) si sottraggono alla regola della rimproverabilità *ex* art. 27, comma 1, Cost.".

[54] Così, Manna (2004), p. 22; Manna, Di Florio (2019), p. 897.

[55] Bricola (2007), p. 588.

[56] Cass. Pen., Sez. III, 9.7.2004, n. 30134. Ulteriori pronunce (Sez. III, 18 febbraio 2014, n. 7504; Sez. V, 14 ottobre 2009, n. 40078 e Sez. III, 15 giugno 2012, n. 23798) hanno ribadito l'orientamento per il quale si sarebbe in presenza di una condizione obiettiva di punibilità intrinseca e ciò essenzialmente perché il reato in questione (la cui condotta tipica consiste già nel trattamento illecito di dati personali) è già offensivo dell'interesse protetto a prescindere dall'effettivo nocumento. Secondo questa giurisprudenza, ritenere il nocumento come evento costitutivo del reato determinerebbe una notevole riduzione del campo applicativo della norma in quanto si dovrebbe necessariamente provare la presenza del dolo intenzionale; il nocumento – in carenza di una esplicita indicazione normativa – può riguardare anche soggetti terzi diversi da quelli titolari dell'interesse alla *privacy* oggetto di tutela penale.

[57] In giurisprudenza, la Corte di Cassazione (in part., Cass. Pen., Sez. III, 9.7.2004) ha escluso che la condizione obiettiva di punibilità possa essere integrata sia in presenza di mere irregolarità formali o procedimentali, quanto in presenza di "*inosservanze che producano un 'vulnus' minimo all'identità personale del soggetto ed alla sua privacy [...] sia nell'aspetto negativo sia positivo e non determinino alcun danno patrimoniale apprezzabile*". Si noti che nel caso di specie, si trattava della utilizzazione di dati personali ricavabili da un elenco di iscritti ad una associazione cui apparteneva lo stesso imputato per scopi elettorali e la Corte di Appello di Messina aveva ritenuto che tale condotta integrasse il reato di trattamento illecito dei dati personali per fini di propaganda politica, condannando l'imputato ex art. 35 L. 675/1996; la Corte di Cassazione ha, in seguito, annullato senza rinvio l'impugnata sentenza ritenendo fondate le doglianze del candidato alle elezioni comunali, ma solo perché nelle more del processo era entrata in vigore la normativa sopravvenuta di cui all'art. 167 Codice della privacy, che, come osservato, introduce la condizione obiettiva di punibilità del nocumento e che impone dunque un accertamento circa la derivazione di un apprezzabile *vulnus* alla persona offesa, non potendosi più sostenere la sussistenza di un reato di pericolo astratto o presunto; sul punto, si veda Palamara (2005), p. 1898.

A tal proposito, appare significativo il rapporto – anche per l'affinità degli interessi tutelati – che sussiste con il reato di rivelazione di segreti di ufficio di cui all'art. 326 c.p. (su cui anche nt. 17), il quale non richiederebbe, quale condizione di punibilità la sussistenza di un danno, ma la mera violazione dei doveri di ufficio: il reato *de quo* è stato, tuttavia, definito dalla giurisprudenza come reato di "*reato di pericolo effettivo e non meramente presunto nel senso che la rivelazione del segreto è punibile, non già in sé e per sé, ma in quanto suscettibile di produrre nocumento a mezzo della notizia da tenere segreta*", Cass. SS.UU., 27.10.2011, n. 4694.

mere funzioni del Garante), con l'obiettivo di superare in questo modo le censure di violazione del principio di legalità, pur sollevando contestualmente questioni di non poco momento sul piano del rispetto del principio di colpevolezza[58].

La condizione obiettiva di punibilità del nocumento si profilava dunque quale spartiacque del momento in cui la condotta – di per sé già illecita e lesiva degli interessi tutelati – assume quel carattere che legittima l'intervento del diritto penale. Infatti, con l'avverarsi della condizione, vi sarebbe – si afferma, non più solo *meritevolezza*, ma altresì – *bisogno di pena*[59], secondo una progressione criminosa sul piano dell'offesa, nel senso che la condotta violatrice del precetto extrapenale, a cui rinvia la norma incriminatrice, può essere punita con la sanzione penale – secondo una scelta di opportunità di natura politico-criminale – soltanto qualora dalla violazione *derivi*, quale conseguenza dell'azione, un *nocumento*: quest'ultimo quindi, a ben vedere, rivelerebbe la sua natura intrinseca rispetto al bene giuridico tutelato.

L'intervento riformatore – in questa occasione non imposto da alcun provvedimento comunitario – ha tentato di ricondurre il fuoco dell'incriminazione, attraverso il recupero dell'offensività del tipo delittuoso, subordinando la punibilità alla lesione del bene individuale della riservatezza e del controllo dei dati personali.

Sennonché, a ben vedere, l'intero sistema di tutela della *privacy*, costituito altresì da numerosi sanzioni di natura amministrativa[60], alcune delle quali costruite specularmente alla fattispecie di cui all'art. 167, ruota attorno all'istituzione di una nuova *Authority*, il c.d. Garante per la protezione dei dati personali, in qualità di autorità di controllo designata anche ai fini dell'attuazione del Codice della *privacy*[61].

In questo senso, può dunque giustificarsi la procedibilità d'ufficio del reato di trattamento illecito dei dati personali, unitamente agli altri illeciti penali, così da non lasciare alla disponibilità privata l'attivazione della giurisdizione penale. In questo schema di tutela sembrerebbe allora individuarsi una "*seriazione degli interessi da tutelare*"[62], in cui la protezione della vita privata del singolo è il "*bene strumentale*", mentre "*bene finale*" sarebbe proprio l'interesse alla sicurezza dei dati, ovvero all'efficientismo dell'ordinamento settoriale facente capo al Garante"[63].

Alla luce di dette considerazioni, la tecnica legislativa prescelta per la formulazione delle disposizioni penali, a ben vedere, all'interno dell'intero quadro normativo soffriva ancora di scarsa chiarezza ed intellegibilità, così da spingere verso una rivisitazione normativa che fosse adeguata alle moderne esigenze di tutela nel mondo dell'informatizzazione dei servizi e delle attività, secondo le linee riformatrici dettate dal Regolamento 2016/679/UE del Parlamento Europeo e del Consiglio del 27 aprile 2016 "*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*", che abroga la precedente Direttiva 95/46/CE.

[58] Sulla problematica coesistenza tra condizioni di punibilità intrinseche e principio di colpevolezza, altresì D'Ascola (1993), pp. 681, che, rifiutando una distinzione tra condizioni intrinseche ed estrinseche, sostiene che tutte le condizioni perseguono interessi estranei all'offesa tipica.

[59] M. Romano (1992), p. 39 s.; altresì, in questi termini, Manna (2004), p. 23. Cfr., in giurisprudenza, Cass. Pen., Sez. III, 17 febbraio 2011, n. 17215, Rv 249991, secondo cui "*il reato è perfetto quando la condotta si sostanzia in un trattamento dei dati personali, in violazione di precise disposizioni di legge, effettuato con il fine precipuo di trarne un profitto per sè o per altri o di recare ad altri un danno ma la sua punibilità discende dalla ricorrenza di un effettivo "nocumento" (nel senso, cioè, che il profitto conseguito o il danno causato siano apprezzabili sotto più punti di vista). Si è, in altri termini, al cospetto di un reato di pericolo effettivo e non meramente presunto [...], con il risultato che la illecita utilizzazione dei dati personali è punibile, non già in sè e per sè, ma in quanto suscettibile di produrre nocumento (cosa che, ovviamente, deve essere valutata caso per caso) alla persona dell'interessato e/o al suo patrimonio*". Cfr,, tuttavia sul punto Pagliaro (2003), p. 502, secondo cui la nozione dogmatica di perfezione del reato richiede l'integrazione di tutti gli elementi previsti per la rilevanza della condotta incriminata(dunque anche la condizione obiettiva di punibilità) e si distingue dalla consumazione che, invece, indica il momento in cui la realizzazione stessa raggiunge, nel suo contenuto concreto, la maggiore gravità. Sulla distinzione, invece, tra perfezione ed efficacia del reato, cfr. M. Gallo (1951), p. 24.

[60] In questa sede, seppur di notevole rilevanza, non ci sofferma sul problematico rapporto tra gli illeciti amministrativi e penali nella materia della *privacy*, per il quale si rinvia a Manes, Mazzacuva (2019), 176.

[61] Si può vedere il sito internet dedicato su: https://www.garanteprivacy.it . Si veda in letteratura, per tutti, per i profili più attuali di rilievo, Troncone (2011), p. 74 s.

[62] cfr. Fiorella (1990), p. 797.

[63] Cfr. ampiamente, *infra* par. 4.1. Si veda Manna (2004), p. 26 sosteneva, a tal proposito, che il "*mantenimento della procedibilità d'ufficio nelle ipotesi in esame, conferma, pertanto la natura anfibia di detti illeciti, in bilico tra la tutela di mere funzioni e la protezione di un assai più pregnante bene giuridico individuale*".

4. La nuova fattispecie di trattamento illecito dei dati personali

La riforma intervenuta con il GDPR – che viene indicato con l'acronimo "GDPR" (*General Data Protection Regulation*), entrato ufficialmente in vigore nell'area UE il 25 maggio 2018[64] – ha cristallizzato in modo definitivo la prevalenza dello strumento amministrativo, nell'ottica del doppio binario sanzionatorio, secondo gli auspici del legislatore europeo, attraverso "*l'imposizione di sanzioni penali per violazioni di […] norme nazionali e di sanzioni amministrative*", le quali, tuttavia, *"non dovrebbe essere in contrasto con il principio del* ne bis in idem *quale interpretato dalla Corte di giustizia*"[65], alla luce di un "*un sistema che preveda sanzioni effettive, proporzionate e dissuasive*"[66].

Il GDPR ha introdotto molte innovazioni – per lo più sconosciute anche ai più moderni ordinamenti giuridici occidentali nel campo della protezione dei dati personali – nel senso di una rimodulazione dell'intero sistema di controllo e gestione dei flussi di informazioni e dati all'interno del mondo digitale.

Tralasciando gli svariati aspetti di natura extrapenale[67] – e nell'ottica di valutare l'esito della trasposizione in Italia degli illeciti penali in materia[68] – va preliminarmente evidenziata l'anomalia di un Regolamento europeo che interviene con uno strumento di diretta applicazione nella materia penale, in apparente violazione dell'art. 83, par. 2 TFUE[69]. Infatti, l'art. 84 del GDPR prescrive l'adozione di sanzioni penali, auspicando altresì l'adozione di misure ablative[70], per le violazioni delle disposizioni tanto dello stesso regolamento quanto delle disposizioni nazionali da adottarsi in virtù di quest'ultimo, laddove, in linea generale, il diritto europeo imporrebbe l'adozione dello strumento legislativo della Direttiva – di applicazione solo mediata – per l'armonizzazione in materia penale[71].

È noto, d'altronde, che il potere legislativo in materia penale spetta agli Stati membri che si sono riservati la piena potestà punitiva: in tal senso, l'art. 83, par. 2 riconosce una competenza penale c.d. accessoria[72] all'UE solo per l'individuazione di "*norme minime relative alla definizione dei reati e delle sanzioni*", le quali "*possono essere stabilite [solo] tramite direttive*".

L'incompatibilità dello strumento prescelto, il regolamento, rispetto alla materia penale è stato solo in parte superato con la prescrizione di un ampio termine per la sua entrata in vigore, che potesse consentire agli Stati membri di adeguarsi e dotarsi degli strumenti necessari, secondo una modalità attuativa tipica delle Direttiva. In questo senso, si è ritenuto che il GDPR, quanto ai suoi effetti, si configuri come una "quasi direttiva"[73].

Orbene, in Italia, il legislatore delegato ha inteso dare attuazione al Regolamento europeo con il D. Lgs. 101/2018 recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*". L'intervento legislativo incide notevolmente sullo schema normativo del Codice della Privacy attraverso la soppressione di numerose disposizioni e l'introduzione di nuove prescrizioni, in un quadro di tutela multilivello in cui l'elemento caratterizzante è costituito dall'eterointegrazione delle norme attraverso un espresso rinvio di cui all'art. 1 del Codice che sancisce che "*il trattamento dei dati personali avviene secondo le norme del regolamento (UE) 2016/679 e del presente codice, nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona*".

[64] In generale, Pisapia (2018), in part. p. 119 s.
[65] GDPR, Considerando n. 49.
[66] GDPR, Considerando n. 152 e altresì Art. 84.
[67] Sui quali si rinvia ampiamente alle *guidelines* del Garante della Privacy, *Guida al nuovo regolamento europeo in materia di protezione dei dati personali*, 2016; in letteratura, tra gli altri, Pizzetti (2016); Bolognini *et al.* (2016).
[68] Si v. da ultimo l'opera di Manes, Mazzacuva (2019), p. 171 s. Sui profili di armonizzazione legislativa del Codice della *Privacy* in materia penale, si v. ampiamente D'Agostino (2019), in part. 29 ss.
[69] Art. 83, par. 2, Trattato sul Funzionamento dell'Unione Europea, dispone che "*allorché il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri in materia penale si rivela indispensabile per garantire l'attuazione efficace di una politica dell'Unione in un settore che è stato oggetto di misure di armonizzazione, norme minime relative alla definizione dei reati e delle sanzioni nel settore in questione possono essere stabilite tramite direttive*".
[70] Considerando n. 49 "*[…] Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente regolamento*".
[71] Come è avvenuto ad esempio in ipotesi di obbligo di incriminazione dei fatti di riciclaggio attraverso lo strumento della direttiva: l'ultima in ordine cronologico è la Quinta Direttiva Antiriciclaggio 2018/843.
[72] Bernardi (2012), p. 43 s.
[73] Cfr. Lamanuzzi (2017), p. 250.

In questo quadro, deve dunque inserirsi il tentativo di correggere gli errori di tecnica legislativa nella disciplina del reato di "*illecito trattamento dei dati personali*", in cui il legislatore segna il passaggio definitivo verso un'architettura penalistica volta ad una *tutela rafforzata* dell'intero sistema *privacy*, che assume definitivamente carattere pubblicistico, nonostante il disvalore di evento si appunti *strumentalmente* sul nocumento agli interessi di un privato[74].

L'art. 167 del Codice della privacy – recante "*Trattamento illecito dei dati personali*" – apre il Capo II del Codice dedicato agli "*Illeciti penali*" e sancisce che *"salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi"*[75].

Se, dunque, il cammino verso l'incriminazione del trattamento illecito dei dati personali sembrava essere segnato da un approccio legislativo in cui la punibilità è sottoposta ad una *doppia selezione* delle condotte meritevoli di sanzione, sia con riguardo all'aspetto subiettivo (con l'individuazione del dolo specifico[76]) che a quello oggettivo (con la previsione della condizione obiettiva di punibilità intrinseca), il legislatore del 2018 ha ulteriormente ristretto l'area del penalmente rilevante. Tale obiettivo è stato perseguito, per un verso, attraverso un'*abrogazione parziale* della norma, nella parte relativa alle condotte di trattamento poste in essere senza il consenso[77] e, per altro verso, attraverso una *tecnica legislativa* che sembra rimarcare,

[74] Cfr. Fiorella (1990), p. 797.

[75] A ben vedere, la norma – seppur rubricata trattamento illecito di dati personali – non fa più espresso riferimento alla modalità commissiva del *trattamento*, limitandosi a descrivere il precetto come mera *operazione* in violazione di una norma extrapenale. *Prima facie*, Si può notare che, per un verso, la fattispecie apparentemente ne beneficerebbe in termini di maggiore chiarezza, non dovendosi altresì accertare i tratti caratteristici del *trattamento dei dati personali*. Per altro verso, si noti che in precedenza era necessaria una condotta commissiva, secondo la descrizione (ora abrogata) dell'art. 4 lett. a) del Codice della privacy (nel senso che nel definire il concetto di "trattamento" l'art. 4 facesse riferimento a condotte attive, Troncone (2011), p. 132; Manna (2010), p. 779 ss.; Contaldo e Marotta (2004), p. 142 s.). Peraltro, a ben vedere, non sembra agevole individuare la ragione dell'espunzione dell'espressione del *trattamento dei dati* dalla formulazione del reato, che, al contempo, ne mantiene intatta la rubrica. Si potrebbe forse sostenere che la *ratio* del legislatore sia stata quella di contemplare anche l'ipotesi di commissione del reato attraverso una condotta omissiva: ad esempio, si pensi alla mancata cancellazione di un dato personale o mancata vigilanza nella trasmissione o gestione degli stessi. Sulla interpretazione giurisprudenziale della condotta di *trattamento*, si veda ad es. Cass. Pen., Sez. III, 16 maggio 2013, n. 29071, secondo cui "il reato di trattamento illecito di dati personali non è integrato se il trattamento dei dati avvenga per fini esclusivamente personali, senza una loro diffusione o destinazione ad una comunicazione sistematica" (ciò derivava, però, dalla clausola limitativa di cui all'art. 5, comma 3, secondo cui il trattamento di dati personali se effettuato da persone fisiche per fini esclusivamente personali "è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione", cfr. Celi (2010), p. 311).
La perplessità accresce ulteriormente laddove si volga lo sguardo al comma 2 dello stesso art. 167 che punisce con una pena più severa, ossia con la reclusione da uno a tre anni,"*chiunque, al fine di trarre per sé o per altri profitto, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di ·garanzia ad esso relative ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quaterdecies arreca nocumento all'interessato*": nella fattispecie ora richiamata – e, si noti, sconosciuta alla formulazione precedente del reato – non solo permane l'espressione del trattamento dei dati personali, ma vi è un esplicito rinvio *per relationem* alle prescrizioni del GDPR che riguardano i c.d. dati particolari. Questi ultimi attengono all'origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, o appartenenza sindacale, nonché ai dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9), ovvero ai dati relativi alle condanne penali e reati (art. 10). In questi casi, tuttavia, si rafforza l'esigenza di tutela penale della *privacy*, nella sua accezione più propriamente individualistica volto alla tutela dei dati c.d. particolari.

[76] Nel senso di un dolo specifico "selezionatore", si veda meglio *infra*, par. 4.2.

[77] Ossia quelle previste dagli abrogati art. 23, ai sensi del quale "*il trattamento di dati personali da parte di privati o enti pubblici economici è ammesso solo con il consenso espresso dell'interessato*", e 24 "*Casi nei quali può essere effettuato il trattamento senza il consenso*". Siffatta *abrogatio* ripropone la questione della rilevanza del consenso nelle fattispecie di trattamento illecito dei dati personali. Nella precedente formulazione era, invero, pacifico che il consenso del titolare dei dati non si configurasse quale scriminante, ai sensi dell'art. 50 c.p., bensì quale *causa di esclusione delle tipicità del fatto*, ossia elemento negativo della fattispecie, nel senso che la sua assenza era elemento essenziale per l'integrazione del reato (Manna (2004), p. 29). Ora, nel novellato quadro normativo, le sole norme extrapenali a cui si fa rinvio sono l'art. 123 che riguarda i dati relativi al traffico; l'art. 126 sui ai dati relativi all'ubicazione e l'art. 130 relativo alle comunicazioni indesiderate. Le tre disposizioni richiamate – non di semplice lettura, in quanto constano di più commi e prescrizioni – consentono, *in linea di massima*, l'utilizzo dei relativi dati personali soltanto con il *consenso* del contraente o dell'utente. Il consenso, in questi casi, non avrebbe rilevanza scriminante, ma la sua assenza sarebbe elemento essenziale della fattispecie penale. Vi sono però prescrizioni la cui violazione non discende dalla mancanza del consenso, come ad esempio, il comma 1 dell'art. 123 in cui i dati relativi al traffico "*sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica*", che – all'evidenza – postulano una violazione tramite omissione (a prescindere dal consenso); o ancora, l'art. 130, comma 3-*bis*, secondo cui è consentito il trattamento dei dati nei confronti di chi non abbia esercitato il diritto di opposizione, postulando quindi la possibilità di trattamento dei dati a prescindere dal consenso e fintantoché non si abbia prestato il proprio *dissenso* (o si sia revocato il *consenso*, in questo caso da ritenersi implicito, cfr. Troncone (2011), p. 119 s.). Altro discorso, invece, deve essere sviluppato in relazione alla violazione del provvedimento del Garante di cui all'art. 129, relativo alle "*modalità di inserimento e di successivo utilizzo dei dati personali relativi ai contraenti negli elenchi cartacei o elettronici a disposizione del pubblico*", le cui modalità di emissione sono specificamente illustrato dal comma 2 dello stesso articolo: si tratta di una vera e propria normale penale in bianco (cfr. Pagliaro (2003), p. 69, per il quale si ha legge penale in bianco quando la stessa faccia "*rinvio ad un atto normativo di grado inferiore per indicare tutti i contrassegni di un fatto che la legge medesima considera penalmente illecito*").

come si cerca di dimostrare nelle riflessioni che seguono, la stessa impostazione incriminatrice adottata nelle ipotesi in cui il diritto penale – per la tutela di interessi di natura generale – interviene nelle *situazioni di anomalia* nella regolamentazione delle relazioni ed affari tra privati, come avviene, tra le altre, in ipotesi di *patrocinio o consulenza infedele* di cui all'art. 380 c.p.

4.1. *Il* nocumento *come disvalore di evento.*

Nella fattispecie in analisi, la modifica di maggiore rilievo è certamente rappresentata dalla formulazione del *nocumento* in termini di *evento* – e dunque rientrante nella struttura tipica del *reato*[78] – e non più, come visto, di condizione obiettiva di punibilità intrinseca, che sebbene possa partecipare alla caratterizzazione offensiva del fatto incriminato, rimane pur sempre elemento futuro e incerto da cui dipende la punibilità dell'autore del reato.

L'effetto è quello di una ulteriore riduzione dell'area del penalmente rilevante, in quanto – abbandonando l'impostazione incriminatrice precedente che postulava un atteggiamento psicologico per cui era sufficiente la *prevedibilità* del *nocumento* – l'autore deve ora agire volendo e rappresentandosi il risultato dannoso.

Viene dunque costruito un reato di evento, che abbandona ora definitivamente l'impostazione formalistica originaria che subordinava la punibilità ad una mera condotta violatrice dei precetti extrapenali. L'evento di nocumento agli interessi dell'interessato deve essere, per l'appunto, conseguenza necessaria della dolosa violazione dei precetti extrapenali.

Nella riforma legislativa, a ben vedere, sembra confermarsi la strumentalità della sanzione penale per il contrasto al trattamento illecito dei dati personali. Il legislatore penale – pur perseguendo la tutela del bene individuale della riservatezza, consacrato ora altresì con l'inciso del *"nocumento all'interessato"*[79] – attraverso la minaccia della pena, intende, da un lato, presidiare l'interesse generale alla protezione dei dati personali e, dall'altro, salvaguardare le funzioni di controllo e gestione del Garante.

Non v'è chi non veda allora una strettissima affinità con il tipo delittuoso del *patrocinio o consulenza infedele*, che costruisce – in modo del tutto analogo – un reato di evento tutto incentrato sull'elemento del *nocumento agli interessi della parte*. Anche in questa ipotesi delittuosa, vi è il ricorso ad una tecnica legislativa che, punendo la condotta di un *patrocinatore* o *consulente tecnico*[80] trasgressiva di *doveri professionali*, ricollega l'offesa alla verificazione dell'evento del *nocumento agli interessi della parte*[81].

La collocazione sistematica del reato, all'interno del Libro II, Titolo III del codice penale relativo ai "*Delitti contro l'amministrazione della giustizia*", aveva fatto propendere dottrina e giurisprudenza verso la tutela di un'oggettività giuridica di natura pubblicistica, in cui si intende garantire la correttezza e lealtà da parte dei patrocinatori e consulenti tecnici per il regolare funzionamento dell'amministrazione giudiziaria[82]. A sostegno di questa impostazione, si è fatto ricorso, oltre alla collocazione sistematica, altresì alla Relazione ministeriale di accompagnamento secondo cui "*il concetto fondamentale […] è che si debbano reprimere gli abusi dei patrocinatori, considerati nei rapporti con l'amministrazione della giustizia, e solo indirettamente nei rapporti privati con i clienti*"[83].

Invero, a fronte di altri orientamenti dottrinali che, invece, privilegiano una prospettiva privatistica[84] vi è chi, escludendo altresì la natura di reato plurioffensivo, sostiene che la fattispecie sarebbe posta a tutela di un *unico interesse complesso*, individuato nell'interesse proces-

[78] Manes, Mazzacuva (2019), 172.
[79] Manes, Mazzacuva (2019), p. 173, in parziale difformità, secondo cui "le modifiche descritte possono essere giudicate positivamente poiché da un lato la maggiore centralità attribuita al nocumento per l'interessato risulta coerente con una logica di tutela personalistica e, dall'altro, la limitazione dei rinvii ad altre disposizioni attenua i noti problemi di indeterminatezza delle fattispecie in parola".
[80] Cfr. Art. 380 c.p. Si noti, peraltro, che la fattispecie *de qua* costruisce un reato proprio, non dissimilmente da quanto previsto dall'art. 167 Codice Privacy che – a dispetto del riferimento a "*chiunque*" – può essere commesso soltanto dal titolare o dal responsabile del trattamento o da colui il quale è stato da essi autorizzato al trattamento, sul punto cfr. Troncone (2011), p. 109.
[81] Si avverte che in precedenza la giurisprudenza considerava sufficiente qualunque azione od omissione idonea a procurare nocumento agli interessi della parte, secondo una ricostruzione in termini di condizione obiettiva di punibilità, cfr. Cass. Pen., 5 dicembre 1975, in *Riv. Pen.*, 1976, 860. Oggi, tuttavia, dottrina e giurisprudenza sono concordi nel considerare il nocumento quale evento tipico del reato, cfr. Calcagno (2009), p. 276.
[82] Calcagno (2009), p. 276.
[83] Si veda Catenacci *et at.* (2011), p. 552. Cfr. altresì, Fornasari (2017), p. 256.
[84] Fiandaca e Musco (2012a), 418.

sualpenalistico che ricomprende sia quello dell'amministrazione della giustizia sia al contempo quello della parte[85] . Secondo questa impostazione, il privato verrebbe in considerazione solo in quanto parte, ovvero in stretto rapporto con l'amministrazione della giustizia; giacché, ove gli interessi del privato non siano lesi e nemmeno posti in pericolo, non si realizza nemmeno l'offesa all'amministrazione della giustizia: "*Intanto l'amministrazione della giustizia può subire offesa, in quanto sia offesa la parte; e, viceversa, il privato può subire offesa come parte solo in quanto sia lesa o posta in pericolo la corretta amministrazione della giustizia*"[86].

Sicché, appurata la piena sovrapponibilità della struttura tipica tra il reato di trattamento illecito dei dati personali ed il reato di patrocinio o consulenza infedele, l'offesa penalmente rilevante – pur ponendosi in diretta relazione con il privato, titolare del bene individuale – emerge, per converso, solo in quanto sia leso o posto in pericolo l'intero sistema di protezione della *Privacy*, regolato dal Codice e sottoposto alla vigilanza del Garante[87]. Con la conseguenza che, anche nel tipo delittuoso *de quo*, sarebbe possibile individuare un *unico interesse complesso*, individuabile nell'interesse collettivo alla protezione dei dati personali, che è leso o posto in pericolo solo "*in quanto sia offesa la parte*".

Tale assunto, a tacer d'altro, trova definitiva conferma nella previsione – in entrambe le fattispecie criminose – della procedibilità d'ufficio, sicché, nonostante l'evento tipico di danno è ancorato ad un *pregiudizio privato*, all'evidenza la promovibilità dell'azione non è lasciata all'arbitrio della parte offesa, e dunque alla sua disponibilità.

4.2. *Il concetto di* nocumento *al vaglio della giurisprudenza*

L'individuazione del significato da attribuire all'espressione del *nocumento* ha peraltro impegnato la giurisprudenza, che ha tentato di tracciare i confini dell'offensività della condotta di trattamento illecito dei dati personali, distinguendolo anche dal concetto di danno.

È noto, d'altronde, a tal proposito, che per "danno" (anche in senso lessicale) si deve intendere ogni fatto circostanza o azione che "nuoce", sia materialmente che moralmente, e che la parola "nocumento" altro non significa (nella lingua italiana, con chiara derivazione latina) che "atto, o effetto, del nuocere": ne discende la quasi sovrapponibilità dei significati di tali parole[88].

Tuttavia, il significato dunque da attribuire alle due entità deve andare oltre la loro lettera e deve indurre a cercare il senso retrostante nella *ratio* posta alla base del suo inserimento nella fattispecie criminosa di cui si discute.

Già l'introduzione del "nocumento" nella novella legislativa del 2003, sembrava finalizzata ad evitare che la disposizione trovi un'applicazione eccessivamente formale e, quindi, come visto, aveva innanzitutto la funzione di dare "effettività" alla tutela della riservatezza dei dati personali[89].

L'accertamento della sussistenza del nocumento si risolve dunque in una *questio facti*. Innanzitutto, è necessario fissare il *quantum* del nocumento: in alcune pronunce di legittimità viene richiesto, ai fini dell'integrazione del reato secondo la formulazione precedente, che la condotta cagioni un *vulnus minimo all'identità personale del soggetto passivo e alla sua privacy*, in altre si fa riferimento a un *vulnus significativo alla persona offesa*[90].

Così, in un caso di propalazione da parte dell'indagato di informazioni relative alla vita sessuale della persona offesa alla sua nuova compagna, la Suprema Corte ha accertato la verificazione di un nocumento, costituito dal pregiudizio, anche di natura *non patrimoniale* subito

[85] Pagliaro (2003a), p. 178.
[86] Pagliaro (2003a), p. 178.
[87] In relazione al *disvalore di evento* ed alla possibilità di individuare un bene giuridico ultimo ed un bene giuridico prossimo, secondo uno schema di c.d. *seriazione dei beni giuridici*, cfr. Fiorella (1990), p. 797.
[88] Così si esprime la giurisprudenza, per tutte, Cass. Pen., Sez. III, 17 febbraio 2011, n. 17215, Rv 249991.
[89] In tal senso, non è utile sforzarsi nella ricerca di un *discrimen* tra le due parole che non riguardi direttamente la direzione teleologica della disposizione in esame; non appare utile dilungarsi in affannosi tentativi di differenziazione terminologica, per cui il danno sarebbe l'evento naturalistico collegato alla condotta tipica ex art. 40 c.p. ed il nocumento riguarderebbe l'insieme delle conseguenze negative in senso lato, quali, ad esempio, le ripercussioni sgradevoli e disonorevoli che dal fatto possono derivare anche a persone diverse dal soggetto passivo (cfr. Troncone (2011), p. 159); tale prospettazione è, peraltro, ancor meno veritiera adesso alla luce della costruzione del reato con un evento di danno, secondo l'espressione del *nocumento all'interessato*.
[90] Si noti, a tal proposito, che si era profilato un filone giurisprudenziale che – nella vigenza della precedente formulazione – aveva ritenuto che il nocumento "*non è soltanto quello derivato alla persona fisica o giuridica cui si riferiscono i dati, ma anche quello causato a soggetti terzi quale conseguenza dell'illecito trattamento*" (cfr. Cass. Pen., Sez. III, 16 luglio 2013, n. 7504), giacché, sotto questo profilo, si è avuta una *abolitio criminis*, attesa ormai la specificazione del "nocumento all'interessato

dalla persona cui si riferiscono i dati quale conseguenza dell'illecito trattamento[91]. Per converso, in un altro caso, veniva ritenuta l'assenza di nocumento per il fatto di due soci di un'associazione che, senza autorizzazione, avevano pubblicato l'immagine di un altro socio dell'opuscolo della medesima associazione, non avendo individuato alcuna conseguenza pregiudizievole[92]. L'indagine del giudice, non potendosi trovare *ex ante* un sicuro parametro cui riferirsi, deve avere riguardo a tutte le circostanze del caso concreto, come si evince, in altra pronuncia di merito, in cui l'imputato è stato condannato per avere pubblicato, senza il preventivo consenso degli aventi diritto, un necrologio su un sito internet dallo stesso gestito, sull'assunto secondo cui il concetto di nocumento ricomprenderebbe "*tutte quelle forme di fastidio e turbamento subito dalla persona offesa, senza che sia necessario dimostrare una vera e propria lesione di un diritto autonomo e diverso rispetto al diritto di controllare l'uso che si fa dei propri dati personali*"[93]; ovvero ancora in una pronuncia di legittimità si arriva ad accertare la sussistenza di un *nocumento* anche nella "*perdita di tempo nel vagliare mail indesiderate e nelle procedure da seguire per evitare ulteriori invii*"[94]

In definitiva, la giurisprudenza – come visto, onerata del compito di dare concretezza al *Tatbestand* – ha dovuto scontare un disagio di disarmonia concettuale con cui sono stati utilizzati e collocati i requisiti strutturali della fattispecie, con la conseguenza di dovere individuare una autonoma funzione del danno e del nocumento. A tal proposito, i giudici hanno quindi tentato di offrire a ciascuno un preciso contenuto oggettivo di valore e una differente *ratio*: ciononostante, la coesistenza dei due concetti solleva profili problematici altresì sul piano soggettivo, come si cerca di illustrare di seguito.

4.3. *Un caso (unico) di dolo specifico apparente.*

La fattispecie in esame richiede, innanzitutto, la sussistenza del *dolo generico*, nel senso che il soggetto agente deve "*operare*" con un atteggiamento volitivo ed intellettivo tale da volere e prevedere[95] gli elementi di tipicità[96] e dunque tanto la violazione delle disposizioni extrapenali a cui si fa rinvio[97], quanto il *nocumento all'interessato*. In questo senso, il tipo delittuoso *de quo* richiede la coincidenza tra ciò che materialmente si realizza (c.d. *Erfolg*) e ciò che si riflette nella sfera intellettiva e volitiva dell'agente, giacché l'agente deve volere e rappresentarsi – nei limiti tracciati dalla rilevanza giuridica e nei termini descritti dagli elementi del reato – che la sua azione comporti un accadimento esteriore tale da arrecare *nocumento* alla persona titolare dei dati oggetto del trattamento[98].

Oltre al requisito del dolo generico, la formulazione del reato mantiene il dolo specifico, in quanto l'agente deve operare "*al fine di trarre profitto o di arrecare un danno*". Come noto, il dolo in questione deve indicare una volontà ulteriore e diversa rispetto agli elementi di tipicità, nel senso che deve rivolgersi ad una finalità la cui realizzazione non è necessaria ai fini della punibilità e dunque dell'integrazione del fatto di reato. Viene usualmente indicato come *mera intenzione* del soggetto, senza che al contempo risulti violato il principio di materialità del fatto tipico.

Si distinguono usualmente alcune tipologie di dolo specifico, che non è possibile in questa

[91] Cass. Pen., Sez. III, 7 febbraio 2017, n. 29549.
[92] Peraltro, nella stessa pronuncia, si afferma che "*il concetto di nocumento alla persona deve ritenersi ben più ampio di quella di danno comprendendo, qualsiasi effetto pregiudizievole che possa conseguire alla arbitratia condotta invasiva altrui*", Trib. Bari, 3 marzo 2016, n. 327.
[93] Trib. Perugia, 26 giugno 2015, n. 1100.
[94] Nel caso di specie, la Cassazione ha condannato l'amministratore delegato ed il direttore finanziario di una società a cui era stata contestata l'attività di spamming con invio di una newsletter a soggetti che non l'avevano richiesta e che al contempo inviavano mail di protesta al gestore del *database*, Cass. Sez. III, 24 maggio 2012, n. 23798.
[95] Cfr. Pagliaro (2003), p. 278.
[96] Cfr. in tal senso Fiandaca e Musco (2012), p. 373, secondo cui l'art. 47 c.p., stabilendo che il dolo è escluso dall'errore sul fatto che costituisce il reato, implicherebbe che la rappresentazione e la volontà devono avere ad oggetto il "fatto tipico".
[97] Sul punto, è bene precisare che il dolo, nel suo aspetto volitivo e rappresentativo, riguarda il significato assunto dall'elemento normativo nel linguaggio del profano, che consente all'agente di percepire la lesività del proprio comportamento; con la conseguenza che, in ipotesi di qualificazioni extrapenali, non se ne pretende la meticolosa conoscenza del giurista, ma ci si accontenta della approssimativa parallela conoscenza profana; tra gli altri, Brunelli, *Il diritto delle fattispecie criminose*, Torino, 2013, 101.
[98] Nel senso che oggetto del dolo è l'evento significativo, ossia "l'accadere esteriore nel suo significato umano e sociale", Pagliaro (2003), p. 293; in senso conforme, ma facendo riferimento al "fatto tipico", quale oggetto del dolo, cfr. Fiandaca e Musco (2012), p. 373; nel senso, invece, che oggetto del dolo sarebbe l'"evento giuridico", ossia l'offesa all'interesse protetto dalla norma, Delitala (1930), p. 64; nel senso, infine, dell'oggetto del dolo quale "evento naturalistico", cfr. Antolisei (1928).

sede ripercorrere[99]. Giova, peraltro, evidenziare come ad esso si faccia principalmente ricorso in ipotesi di c.d. "*dolo specifico selettivo o differenziatore*", che si ha qualora il fatto risulti già sufficientemente descritto quanto a modalità oggettive, sicché, essendo la condotta oggettiva già offensiva del bene protetto, la finalità *ulteriore* non arreca un contributo nuovo o particolarmente significativo al contenuto dell'offesa[100].

Orbene, il ricorso al dolo specifico era stato inteso originariamente proprio nel senso di selezionare le condotte realmente offensive del bene giuridico tutelato dalla norma *de qua* onde evitare un eccessivo ampliamento dell'area del penalmente rilevante. In effetti, nella costruzione di una fattispecie incriminatrice fondata su elementi meramente *formalistici*, ossia sulla violazione di norme *extrapenali*, il dolo specifico svolgeva il ruolo selettivo delle condotte suscettibili di sanzione penale: in tal senso, soltanto una violazione del Codice della *privacy* che fosse determinata da una *finalità di lucro o di danno* legittimava l'intervento penalistico.

La modifica della struttura del reato che oggi prevede quale *evento* (su cui si appunta il contenuto lesivo ed è dunque, nei profili visti *supra*, oggetto del dolo) la sussistenza del nocumento all'interessato – che configura il tipo quale reato di danno – appare incompatibile con il mantenimento del dolo specifico in funzione di selezione delle violazioni delle prescrizioni richiamate in materia di *privacy*.

Nel caso di specie, la finalità ulteriore perseguita dal soggetto si sovrappone al risultato materiale (*Erfolg*), ossia all'evento naturalistico ed al contenuto offensivo del reato. Si tratta, a ben vedere, di un *dolo specifico di danno apparente*: sarebbe, quantomeno *prima facie*, del tutto superfluo in quanto la finalità o partecipa alla struttura della tipicità, e dunque è necessaria la sua realizzazione esteriore, ovvero è soltanto ulteriore rispetto alla struttura tipica del fatto, con la conseguenza che – nell'esercizio della sua funzione selettiva – individua tra le finalità dell'agente quelle lesive del bene tutelato. Dunque, delle due l'una: la finalità di danno è oggetto del dolo o è ulteriore rispetto alla struttura tipica.

Peraltro, a ben vedere, non risultano, all'interno del sistema penale integrato, altri tipi delittuosi costruiti nei termini qui formulati. L'unico esempio di tal fatta si rinviene nel precedente Codice Zanardelli che nella definizione dell'omicidio doloso conteneva l'inciso "*al fine di uccidere*". Detta formulazione fu tacciata di superficialità tanto da essere soppressa nel progetto preliminare del Codice Rocco, siccome incompatibile con le norme generali sull'elemento soggettivo del reato contenute nel libro primo (II comma dell'art. 42 e 43, prima parte). Anche in quell'ipotesi, si sarebbe potuto parlare di *dolo specifico apparente*, nonostante fosse plausibile una doppia selezione, tanto sul piano oggettivo – con l'accertamento dell'evento infausto – quanto sul piano soggettivo, attraverso la partecipazione della finalità al contenuto offensivo del fatto; e ciò al fine di differenziare l'omicidio doloso dall'ipotesi delittuosa meno grave dell'omicidio preterintenzionale[101].

Orbene, ritornando alla fattispecie qui in esame, è doveroso chiedersi se permanga una – seppure marginale – utilità del dolo di danno, nella sua funzione selettiva delle condotte suscettibili di sanzione penale: d'altronde, appare difficile pensare ad un trattamento illecito dei dati personali che, arrecando un *nocumento*, non sia accompagnato da una tale finalità.

A ben vedere, la formulazione normativa è il frutto di un *iter* legislativo che – nella bozza preliminare – non prevedeva più il dolo di danno, il quale avrebbe lasciato il posto soltanto al dolo specifico di profitto, con una ulteriore riduzione dell'area del penalmente rilevante.

Notevoli e fondate apparivano dunque le critiche rivolte allo *schema di decreto*: meno ragionevole, tuttavia, è stata la novellazione, per i motivi che seguono.

Da un lato, l'eliminazione delle fattispecie di danno e di violazioni non lucrative sembrava diminuire la tutela di fatti incresciosi come il *revenge porn* o lo *slut shaming*[102], che dovrebbero al contrario essere oggetto di attenta tutela.

A tal proposito, il Garante della Privacy europeo riteneva che la sola previsione del dolo specifico di profitto (vantaggio o altra utilità) fosse "*un'involuzione normativa, particolarmente*

[99] Sul tema, ampiamente, per tutti, Picotti (1993); nel senso che il dolo specifico non sia nemmeno una forma di dolo, perché estraneo alla condotta illecita, cfr. Pagliaro (2003), p. 287.

[100] Esempio classico di questa tipologia è la fattispecie del furto in cui il fine di trarre profitto dalla cosa mobile altrui svolge esclusivamente la funzione di selezionare le condotte punibili, dal momento che nella stessa condotta di sottrazione e impossessamento della cosa risulta già insito l'attacco al patrimonio; cfr. Brunelli (2013), p. 113.

[101] Sul punto, cfr. Mantovani (2016), p. 153.

[102] Si tratta di quei fenomeni, ormai molto diffusi, soprattutto tra i giovani, in cui avviene una condivisione online o tramite social di immagini o video intimi (aventi spesso sfondo sessuale) senza il consenso della o del protagonista degli stessi, come forma di vendetta o ritorsione, cfr. Citron e Franks (2014), p. 345.

inadeguata" in quanto "*non idonea ad inglobare al suo interno i fenomeni fortemente lesivi dei diritti alla personalità sorretti dalla coscienza e volontà di trattare dati personali al fine di danneggiare terzi soggetti*"[103]. Similmente, si esprimeva il Garante nazionale il quale propugnava l'inserimento del dolo alternativo di danno "*in ragione dell'esigenza di presidiare con la sanzione penale condotte connotate da un simile disvalore*", al fine peraltro "*di assicurare una maggiore continuità normativa con la fattispecie vigente e di evitare gli effetti (anche sui processi in corso) dell'abolitio criminis che si dovesse ravvisare, in parte qua, per effetto della novellazione proposta*"[104].

Dall'altro lato, nonostante la questione fosse stata correttamente individuata – ossia, la necessità di non lasciare impuniti fatti di grave allarme sociale, come il *revenge porn* o l'utilizzo di immagini e video con finalità di discredito, intimidazione o minaccia, come anche la necessità di assicurare la continuità normativa – la soluzione proposta è stata erroneamente impostata.

Se è vero che il dolo specifico *aggiunge* una finalità ulteriore ai caratteri della fattispecie delittuosa, che ben può sussistere soltanto interiormente nella psiche dell'agente, è altrettanto vero che la nuova formulazione impone una sua manifestazione esteriore, attraverso l'espressione del *nocumento all'interessato*: non solo il soggetto deve agire con siffatta *intenzione di danno*, ma deve ottenere materialmente il risultato (*Erfolg*): si disperderebbe, invero, la funzione selettiva del dolo specifico di danno.

Se, davvero, dunque, si fosse voluto perseguire con efficacia i fatti di maggiore allarme sociale – che il *web* rende ancora più insidiosi – sarebbe stato forse più opportuno espungere del tutto il dolo specifico, tanto di danno quanto di profitto.

Tale soluzione non avrebbe certamente tradito neppure l'auspicio del legislatore di circoscrivere l'area del penalmente rilevante, giacché l'elevazione dell'elemento del *nocumento* ad evento del reato, coperto dal fuoco del dolo, senza alcuna selezione delle condotte sorrette dal dolo specifico di profitto e di danno, eviterebbe, per un verso, l'incongruità[105] di una duplicità della finalità di danno e, per altro, garantirebbe comunque la continuità normativa. In quest'ultimo senso, si eviterebbe altresì, a ben vedere, la temuta *abolitio criminis*, in quanto sussisterebbe ancora un'analogia strutturale del reato *pre* e *post* riforma, atteso che identici sarebbero gli elementi materiali e che, venendo meno *in toto* la funzione selettiva del dolo specifico, si riespanderebbe, piuttosto che ridursi, l'area del penalmente rilevante[106].

Il legislatore ha, ciononostante, mantenuto entrambe le forme di dolo specifico.

Ne discenderebbe peraltro, a ben vedere, il pericolo di una *interpretatio abrogans* del *dolo specifico di danno*. Onde evitare siffatto esito, una soluzione ermeneutica di 'compromesso' – nell'ottica di attribuire un significato all'intenzione del legislatore, secondo una interpretazione teleologica – potrebbe forse prendere spunto da quanto avveniva con l'omicidio volontario sotto la vigenza del Codice Zanardelli[107]: il *dolo di danno* avrebbe dunque l'effetto di configurare il reato come reato a dolo intenzionale (e non specifico), qualificazione che si identifica nella direzione della volontà alla verificazione dell'evento, che si realizza secondo l'intenzione; pertanto, la previsione del dolo di danno renderebbe inapplicabile il reato di trattamento illecito quando la condotta sia sorretta da un dolo eventuale ovvero indeterminato[108].

La conseguenza è allora quella di una – inconsapevole – restrizione dell'area del penalmente rilevante adesso verificatasi sul versante soggettivo, il che in definitiva finirebbe col frustrare le esigenze di tutela prospettate dal Garante.

E a ben vedere, infine, se davvero la *ratio legis* fosse stata quella di tutelare il bene giuridico individuale della riservatezza, il reato di cui all'art. 167 sembra divergere dagli altri modelli delittuosi in cui il legislatore tutela la sfera privata senza subordinare la punibilità ad un dolo specifico di danno. Basti pensare, a titolo esemplificativo, alla ipotesi di cui all'art. 620 c.p., in cui si punisce la *Rivelazione del contenuto di corrispondenza, commessa da persona addetta al servizio delle poste, dei telegrafi o dei telefoni*, che è reato di mera condotta di rivelazione, senza alcuna selezione delle intenzioni criminose; ovvero al reato di *Rivelazione del contenuto di documenti segreti* di cui all'art. 621 c.p., in cui – premessa la punibilità per la mera condotta di

[103] Le opinioni del Garante *Privacy* europeo allo schema del decreto si possono visualizzare sul sito web https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9163359

[104] Cfr. sulle opinioni del Garante *Privacy* italiano allo schema del decreto, vedi altresì nt. precedente.

[105] Cfr. Manna (2004), p. 22. Cfr. *supra* par. 3.

[106] Cfr. Cass. SS.UU., 16 giugno 2003, n. 25888, Rv. 224607.

[107] Ramacci (2016), p. 43.

[108] Manes, Mazzacuva (2019), 173, secondo cui "la finalità dell'agente, coincidendo con l'oggetto del dolo generico, dif fatto lo qualifica come *intenzionale*". Inoltre, possono rinvenirsi simili riflessioni con riguardo ai reati tributari con dolo specifico, per i quali, si veda, per tutti, Salcuni (2001), p. 131 s.

rivelazione – viene aggiunta una ipotesi di impiego subordinata, tuttavia, ad un dolo specifico "*a proprio o altrui profitto*" e alla condizione obiettiva di punibilità del *nocumento*.

5. Il nuovo fuoco della tutela penale del trattamento illecito dei dati personali

Proseguendo nell'analisi della complessa formulazione della tutela penale in materia, ci si avvede che il vero fuoco di essa si rinviene ora in due nuovi tipi delittuosi introdotti da ultimo agli art. 167-*bis* "*Comunicazione e diffusione illecita di dati personali riferibili a un rilevante numero di persone*" e 167-*ter* "*Acquisizione fraudolenta di dati personali*"[109]. Di una tale rilevanza delle figure menzionate è indicatore la relativa previsione di un trattamento sanzionatorio più severo rispetto alla fattispecie base dell'art. 167 del Codice *privacy*[110].

L'art. 167-*bis* punisce due condotte materiali che sono definite dal nuovo art. 2-*ter* del Codice, ossia la *comunicazione* e la *diffusione*. Queste due modalità di manifestazione differiscono soltanto con riguardo ai soggetti destinatari, che astrattamente verrebbero a conoscenza dei dati personali: mentre nella comunicazione i destinatari sono determinati, al contrario nel caso della diffusione i destinatari sono invece indeterminati[111]. Elemento essenziale della nuova fattispecie di reato è che la condotta si riferisca ad un "*archivio automatizzato o a una parte sostanziale di esso contenente dei dati personali oggetto di trattamento su larga scala*".

In questa espressione viene, innanzitutto, evocato per la prima volta quale oggetto del reato un "*archivio automatizzato*", del quale però non si rinviene alcuna definizione nel Codice della Privacy. A ben vedere, il termine rimanda ad una nozione di natura informatica e digitale, la cui effettiva comprensione richiede avanzate conoscenze tecniche. L'art. 4, n. 6 del GDPR definisce un "*archivio*" come "*qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico*". In attesa di una elaborazione giurisprudenziale in proposito, si può sostenere che l'attributo "automatizzato" faccia riferimento ad un insieme di dati la cui elaborazione e gestione sia sottoposta ad automatismi computazionali svincolati da un diretto ed immediato coinvolgimento di una persona fisica.

In via esemplificativa, si potrebbe pensare al noto fenomeno della c.d. *profilazione*, che emerge anche normativamente dall'art. 22 del GDPR, secondo cui "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.*"

Da questo punto di vista, si comprenderebbe l'altra espressione – anch'essa sconosciuta nel panorama penalistico – del "*trattamento su larga scala*", che, ad ogni buon conto, solleva evidenti questioni di tassatività del precetto penale secondo una tecnica legislativa che ricalca i paradigmi di una legislazione simbolica ed emergenziale. In definitiva, vengono lasciati ampi margini di discrezionalità all'opera ermeneutica del giudice, al quale viene demandato l'onere di provvedere alla sua efficienza pratica, colmando l'indeterminatezza e genericità dell'espressione del "*trattamento su larga scala*"[112]. Spetterà, dunque, al giudice individuare il momento in cui avviene la lesione al bene giuridico tutelato – che legittima l'intervento della sanzione penale – ed individuabile, nel caso di specie, nel diritto dei *consociati* ossia della collettività (e non più del singolo o, meglio, del diretto "interessato") al corretto utilizzo dei dati personali, con particolare riguardo ai sistemi informatizzati e automatizzati.

Peraltro, non appare peregrino evidenziare che l'espressione *de qua* è anch'essa frutto di un *iter* legislativo complesso, tanto perché si inserisce all'interno del sistema di tutela multilivello del GDPR e dell'eterointegrazione normativa in materia, quanto perché il reato di nuovo

[109] Cfr. per un primo commento sulle nuove disposizioni penali altresì, D'Agostino (2019), in part. 42 ss.
[110] L'art. 167-*bis* prevede la pena della reclusione da uno a sei anni, mentre l'art. 167-*ter* prevedono la pena della reclusione da uno a quattro anni.
[111] Si tenga presente, peraltro, che le due espressioni erano già presenti nella fattispecie base dell'art. 167 ("*se il fatto consiste nella comunicazione o diffusione*"). A tal proposito, in dottrina, si riteneva che – vigente la precedente formulazione – per punire la comunicazione e diffusione non occorresse la derivazione del nocumento, in quanto la mancata previsione normativa faceva suppore che il potenziale diffusivo della divulgazione del dato o dei dati sia di per sé solo sufficiente a garantire la punibilità del fatto, senza la concretizzazione della condizione di un effettivo danno, cfr. Manna (2005), p. 257.
[112] Cfr. Resta (2019), p. 1037.

conio, nell'*intentio legis* di colpire condotte di recente emersione[113], è il risultato di rilevanti emendamenti. Originariamente, la condotta lesiva era descritta attraverso il ricorso ad espressioni di altrettanta indeterminatezza, laddove il momento dell'offesa si sarebbe verificato qualora il trattamento si fosse riferito "*ad un rilevante numero di persone*".

A seguito di opinioni dissenzienti da parte del Garante della Privacy[114], sia italiano che europeo, si è tentato di individuare un criterio che non facesse solo leva sul criterio quantitativo, ma avesse anche una qualche valenza qualitativa. La scelta incriminatrice, tuttavia, ha mantenuto il riferimento ad una nozione di natura quantitativa: a ben vedere, non sussisterebbe alcuna differenza sostanziale tra un "*rilevante numero di persone*" ed "*un trattamento su larga* scala". Sarebbe stato senz'altro più coerente con l'intero sistema di tutela qualificare la condotta in termini invece qualitativi, nel senso di collegarla alla comunicazione o diffusione di dati personali c.d. particolari, ossia giudiziari e sensibili (di cui all'art. 2-*sexies*).

Sulla fattispecie *de qua* grava dunque un'ipoteca di illegittimità costituzionale per violazione del principio di tassatività e sufficiente determinatezza del precetto, quale corollario del principio di legalità.

Come anticipato, l'altra nuova incriminazione – che, nel sistema di tutela integrato, rende ulteriormente marginale la fattispecie base del trattamento illecito dei dati personali – è costituito dal nuovo art. 167-*ter* che, "*salvo che il fatto non costituisce più grave reato*" punisce con la reclusione da uno a quattro anni "*chiunque, al fine trarne profitto per sé o altri ovvero di arrecare un danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala*".

Anche in questa ipotesi delittuosa permane un dolo specifico di profitto e danno, in funzione selettiva delle condotte realmente offensive, ma al contempo viene formulato un reato di mera condotta, consistente nell'acquisizione fraudolenta, che è già perfetto a prescindere dall'accertamento di un nocumento. Da questo punto di vista, anche in questo tipo delittuoso, la tutela dal bene-categoria individuale della *privacy* non rileva ai fini della punibilità, se non nei limiti in cui viene riproposto un dolo specifico di danno, il quale, tuttavia, come noto, non deve verificarsi ai fini dell'integrazione del reato. La *ratio* dell'incriminazione si può allora rintracciare nell'interesse generale dei consociati ad una tutela rafforzata dei sistemi automatizzati, il cui utilizzo fraudolento deve essere presidiato da una sanzione penale.

Le due fattispecie delittuose si allontanano definitivamente dai profili privatistici ed individualistici del bene-categoria della *privacy*, che rimane soltanto sullo sfondo e la cui offesa non rileva neppure in termini di tipicità, come nell'ipotesi base dell'art. 167, secondo la struttura di reato di danno. Ebbene, in altri termini, nell'ottica di massima efficienza del nuovo modello di protezione dei dati personali auspicato dal legislatore europeo, il disvalore penale non risiede più nella lesione di un bene individuale, che può ben concretizzarsi nell'accertamento del *nocumento all'interessato*.

Invero, la lesione è rivolta ad una nuova e più pregnante oggettività giuridica – prima sconosciuta, e di nuova emersione alla luce dei nuovi utilizzi dei mezzi informatici e digitali – inquadrabile nell'*interesse generale dei consociati al corretto utilizzo delle piattaforme digitali, contenitori automatizzati di innumerevoli dati personali*: queste ultime – nell'ottica di una maggiore efficienza del sistema integrato di tutela – necessitano di un controllo giuridico più stringente, che può giungere anche all'inflizione della sanzione penale.

Il ragionamento dunque appare conforme agli auspici del legislatore europeo che ha imposto agli Stati membri di fare ampio ricorso alla sanzione amministrativa, la quale, nel rispetto del principio di sussidiarietà, deve cedere il posto a quella penale soltanto nelle ipotesi di maggiore allarme sociale. E sol che si ponga mente alle potenzialità lesive dei sistemi informatizzati e digitalizzati, ci si avvede della necessità di un presidio penale. In questo senso, la scelta incriminatrice sembra adeguata alla tutela del *sistema di protezione dei dati personali*, che assurge oggi – alla luce degli art. 167 s. Codice della Privacy – a nuovo bene-categoria di natura pubblicistica. Rimane tuttavia la perplessità di un ricorso ad elementi vaghi, come gli "*archivi automatizzati*" o ancora "*il trattamento su larga scala*", la cui concretizzazione spetterà all'attenta opera ermeneutica del giudice.

[113] Si pensi, tra gli altri, al celebre scandalo di *Cambridge Analytica*; cfr. *Carol Cadwalladr*, *The Cambridge Analytica file*, in *The Guardian*, 18 marzo 2018.
[114] Cfr. sul sito del Garante della privacy, cfr. *supra* nt. 103.

Bibliografia

Angioni, Francesco (1989), "Condizioni di punibilità e principio di colpevolezza", *Rivista Italiana di Diritto e Procedura Penale*, 1440 ss.

Angioni, Francesco (1994), *Il pericolo concreto come elemento della fattispecie penale: la struttura oggettiva* (Milano, Giuffrè).

Antolisei, Francesco (1928), *L'azione e l'evento nel reato* (Milano, Istituto Editoriale scientifico)

Antolisei, Francesco (2003) *Manuale di diritto penale. Parte Generale* (Milano, Giuffrè)

Bernardi, Alessandro (2012), *La competenza penale accessoria dell'Unione Europea: problemi e prospettive*, *Diritto penale contemporaneo – Rivista trimestrale*, 1, pp. 43 ss.

Bolognini, Luca, Pelino, Enrico, Bistolfi, Camilla (2016), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali* (Milano, Giuffrè).

Bricola, Franco (1967), *Prospettive e limiti della tutela penale della riservatezza*, *Riv. it. dir. proc. pen.*, pp. 1114 ss.

Bricola, Franco (2007), *Punibilità (condizione obiettive di)*, in *Noviss D.I.*, Torino, Giappichelli, 588 ss.

Brunelli, Ivan (2013), *Il diritto delle fattispecie criminose*, II Ed. (Torino, Giappichelli).

Calcagno, Elisabetta (2009), *Reati contro l'amministrazione della giustizia*, Vol. 7, (Giuffrè, Milano).

Canestrari, Stefano (1991) "Reato di pericolo", *Enc. Giur. Treccani*, XXVI, pp. 7 ss.

Carnelutti, Francesco (1955) "Diritto alla vita privata (Contributo alla teoria della libertà di stampa)", *Riv. trim. dir. pubbl.*, 4, 3 ss.

Catenacci, Mauro *et al.* (2011), *Reati contro la pubblica amministrazione e contro l'amministrazione della giustizia*, in *Trattato teorico-pratico di diritto penale*, diretto da Palazzo, Francesco, Paliero, Carlo Enrico (Torino, Giappichelli).

Celi, Loredana (2010), "Il ruolo del limite espresso dall'art. 5, comma 3, del d.lg. n. 196/2003 nella struttura del delitto di trattamento illecito di dati personali", *Cass. Pen.*, 1, pp. 311-319.

Citron, Danielle Kitts, Franks, Mary Anne (2014), "Criminalizing revenge porn", *Wake Forest Law Review*, 49, pp. 345 ss.

Contaldo, Alfonso, Marotta, Egidio (2004), "Depenalizzazione e nuove tutele dei dati personali anche alla luce del Codice della Privacy (d.lgs. 30 giugno 2003, n. 196)", *Giur. merito*, pp. 142 ss.

Corrias Lucente, (1997), "Sanzioni penali e amministrative a tutto campo per aumentare la tutela del cittadino", *Guida dir.*, 4, pp. 82.

D'Agostino, Luca (2019), "La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101", *Archivio Penale*, fasc. 1.

D'Ascola, Vincenzo Nico (1993), "Punti fermi i aspetti problematici delle condizioni obiettive di punibilità", *Rivista Italiana di Diritto e Procedura Penale*, pp. 652-681.

Delitala, Giacomo (1930), *Il fatto nella teoria generale del reato* (Padova, Cedam).

Dolcini, Emilio (2000): "Responsabilità oggettiva e principio di colpevolezza", *Rivista italiana di diritto e procedura penale*, pp. 863-882.

Fiandaca, Giovanni, Musco (2012), *Diritto penale. Parte Speciale*, Vol. I, V ed. (Milano, Giuffrè)

Fiore, Stefano (1999), voce *Riservatezza (diritto alla)*, IV, *Enc. giur. Treccani*, Roma.

Fiorella, Antonio (1990) voce *Reato. Il reato in generale (diritto penale)*, in *Enc. Dir.*, XLII, pp. 770-816.

Fornasari, Gabriele (2017), "Patrocinio o consulenza infedele", in Fornasari, Gabriele, Riondato, Silvio (a cura di), *Reati contro l'amministrazione della giustizia* (Torino, Giappichelli), pp. 256 ss.

Galdieri, Paolo (2012), "Il trattamento illecito del dato personale nei social network", *Giur. mer.*, 12, pp. 2697.

Gallo, Marcello, *Il concetto unitario di colpevolezza* (Milano, Giuffrè).

Giunta, Fausto (1997), "Il diritto penale dell'ambiente in Italia: tutela di beni o tutela di funzioni?", *Rivista Italiana di Diritto e Procedura Penale*, pp. 1102 ss.

Grasso, Giovanni (1986)"L'anticipazione della tutela penale: i reati di pericolo e i reati di attentato",", *Rivista Italiana di Diritto e Procedura Penale*, pp. 689 ss.

Insolera, Gaetano, Stortoni, Luigi, "Le vicende della punibilità", *Introduzione al sistema penale*, a cura di Insolera, Gaetano, II Ed., (Torino, Giappichelli), pp. 413 ss.

Lamanuzzi, Marta (2017), "Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento UE 2016/679 e nuove responsabilità per gli enti", *Rivista di Scienze Giuridiche*, 1, pp. 221 ss.

Manes Vittorio, Mazzacuva Francesco (2019), "GDPR e nuove disposizioni penali del Codice privacy", *Diritto penale e Processo*, fasc. 2, p. 171 ss.

Manna, Adelmo (1989), *Beni della personalità e limiti della protezione penale*, (CEDAM, Padova).

Manna, Adelmo (1993), "La protezione penale dei dati personali nel diritto italiano", *Rivista trimestrale diritto penale dell'economia*, pp. 179 ss.

Manna, Adelmo (2001), "Il trattamento dei dati personali: le sanzioni penali", in Fiora-vanti, Laura (a cura di), *La tutela penale della persona. Nuove frontiere, difficili equilibri* (Milano, Giuffrè), pp. 339 ss.

Manna, Adelmo (2004), "Codice della privacy: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali", *Diritto penale e processo*, 1, pp. 17-31.

Manna, Adelmo (2005), "Privacy on line: quali spazi per la tutela penale", *Diritto dell'internet*, pp. 257 ss.

Manna, Adelmo (2010), "I soggetti in posizione di garanzia", *Diritto dell'informazione dell'informatica*, pp. 779-794.

Manna, Adelmo, Di Florio, Mattia (2019), "Riservatezza e diritto alla privacy: in particolare la responsabilità per omissionem dell'internet provider", in Cadoppi Alberto, Canestrari Stefano, Manna Adelmo, Papa Michele (a cura di), *Cybercrime* (Milano, Utet), p. 892 ss.

Mantovani, Ferrando (1968), "Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi", *Arch. giur.*, p. 61 ss.

Mantovani, Ferrando (2017), *Diritto Penale. Parte Generale* (Padova, Cedam).

Mantovani, Ferrando (2016) *Diritto Penale. Parte Speciale*, *Delitti contro la persona*, Vol. I (Padova, Cedam).

Marinucci, Giorgio (1987), "Profili di una riforma del codice penale", *Beni e tecniche della tutela penale. Materiali per la riforma del codice* (Milano, Franco Angeli), pp. 19 ss.

Militello, Vincenzo, Spena, Alessandro (2018), *Mobilità, sicurezza e nuove frontiere tecnologiche* (Torino, Giappichelli).

Mucciarelli, Francesco, "Informatica e tutela penale della riservatezza", in Picotti, Lorenzo (2004), *Il diritto penale dell'informatica* (Padova, Cedam), pp. 173 ss.;

Musco, Enzo (1974), *Bene giuridico e tutela dell'onore* (Milano, Giuffrè).

Musotto, Giovanni (1936), *Le condizioni obiettive di punibilità nella teoria generale del reato* (Palermo, Tumminelli).

Nuvolone, Pietro (1955), *Il diritto penale del fallimento e delle altre procedure concorsuali*, (Milano, Giuffrè).

Padovani, Tullio (1984), "La problematica del bene giuridico e la scelta delle sanzioni", *Dei delitti e delle pene*, pp. 114-131

Padovani, Tullio (1987), "Tutela di beni e tutela di funzioni nella scelta tra delitto, contravvenzione e illecito amministrativo", *Cassazione Penale*, pp. 670 ss.

Pagliaro Antonio (1960), *Il fatto di reato* (Palermo, G. Priulla)

Pagliaro, Antonio (1965), "Bene giuridico e interpretazione della legge penale", *Studi in onore di Francesco Antolisei*, pp. 389 ss.

Pagliaro, Antonio (2003), *Principi di diritto penale. Parte generale* (Milano, Giuffrè).

Pagliaro, Antonio (2003), *Principi di diritto penale. Parte Speciale* (Milano, Giuffrè).

Palamara, Luca (2005), "Note in tema di rilevanza penale del trattamento illecito dei dati personali", *Cassazione Penale*, pp. 1898 ss.

Palazzo, Francesco (1975) "Considerazioni in tema di tutela della riservatezza (a proposito del nuovo art. 615-bis c.p.)", *Rivista Italiana di Diritto e procedura Penale*, p. 126 ss.

Parodi Giusino, Manfredi (1999), "La condotta nei reati a tutela anticipata", *Indice Penale*, pp. 687 ss.

Patrono, Paolo (1986), Voce *Privacy e vita personale (diritto penale)*, *Enc. dir.*, XXXV, pp. 557 ss.

Picotti, Lorenzo (1993), *Il dolo specifico. Un'indagine sugli 'elementi finalistici' delle fattispecie penali* (Milano, Giuffrè).

Picotti, Lorenzo (2012), "I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali", *Giurisprudenza di merito*, 12, pp. 2522

Pisapia, Alice (2018), *La tutela per il trattamento e la protezione dei dati personali* (Torino, Giappichelli)

Pizzetti, Franco (2016), *Privacy e diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento* (Torino, Giappichelli).

Pulitanò, Domenico (1987), "La formulazione delle fattispecie di reato: oggetti e tecniche", *Beni e tecniche della tutela penale. Materiali per la riforma del codice* (Franco Angeli, Milano), pp. 33 ss.

Pulitanò, Domenico (1988), "Una sentenza storica che restaura il principio di colpevolezza", *Rivista Italiana di Diritto e Procedura Penale*, pp. 686 ss.

Ramacci, Fabrizio (2016), *I delitti di omicidio* (Torino, Giappichelli).

Resta, Federica (2019), "I reati in materia di protezione dei dati personali", in Cadoppi Alberto, Canestrari Stefano, Manna Adelmo, Papa Michele, *Cybercrime* (Milano, Utet), p. 1019 ss.

Rodotà, Stefano (2005), *Intervista sulla Privacy* (Bari, Laterza).

Romano, Mario (1992), "Meritevolezza di pena", "bisogno di pena" e "teoria del reato", *Rivista Italiana di Diritto e Procedura Penale*, pp. 39 ss.

Romano, Mario (1995), *Commentario sistematico del codice penale*, II Ed. (Milano, Giuffrè), pp. 319 ss.

Salcuni, Giandomenico (2001)," Natura giuridica e funzioni delle soglie di punibilità nel nuovo diritto penale tributario", *Rivista trimestrale diritto penale dell'economia*, pp. 131-187.

Seminara, Sergio (1998), "Appunti in tema di sanzioni penali nella legge sulla privacy", *Responsabilità Civile e previdenza*, pp. 911 ss.

Sgubbi, Filippo (1998), "Profili penalistici della L. 675/1996", *Rivista trimestrale diritto penale dell'economia*, pp. 75 ss.

Troncone, Pasquale (2011), *Il delitto di trattamento illecito dei dati personali* (Torino, Giappichelli).

Troncone, Pasquale (2014), "Il caso Google (e non solo), il trattamento dei dati personali e i controversi requisiti di rilevanza penale del fatto", *Cassazione Penale*, 6, pp. 2066 ss.

Veneziani, Paolo (2001), "I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali", in Fioravanti, Laura (a cura di), *La tutela penale della persona. Nuove frontiere, difficili equilibri* (Milano, Giuffrè), pp. 369 ss.

Vigevani, Giulio Enea (2016), "Diritto all'informazione e privacy nell'ordinamento italiano: regole e eccezioni", *Rivista dell'informazione e dell'informatica*, 3, pp. 473-498.

Warren, Samuel, Brandeis, Louis (1890), "The right to privacy", *Harvard Law Review*, 4, pp. 193-220.

Il compendio sanzionatorio della nuova disciplina privacy sotto la lente del *ne bis in idem* sovranazionale e della Costituzione

El compendio sancionatorio de la nueva regulación de la privacidad bajo la lente del ne bis in idem *internacional y de la Constitución italiana*

The Sanctioning System for Privacy-Related Infringements from the Supranational Ne Bis In Idem *and the Italian Constitution Perspectives*

Ludovica Deaglio
Dottoranda in Diritti e Istituzioni presso l'Università degli Studi di Torino
ludovica.deaglio@unito.it

Abstracts

Il lavoro si propone di analizzare l'impianto sanzionatorio previsto dalla vigente normativa in materia privacy, recentemente oggetto di importanti modifiche a livello comunitario e nazionale. Nell'ambito di una concisa ricostruzione degli illeciti amministrativi e penali oggi previsti dal cd. GDPR e dal Codice Privacy, si evidenziano le criticità connesse alla formulazione normativa dei suddetti illeciti, non sempre di univoca interpretazione. Il Legislatore pare aver adottato il cd. doppio binario sanzionatorio: la seconda parte dell'elaborato è dunque dedicata alla valutazione della compatibilità di tal impostazione con il principio del *ne bis in idem*, così come elaborato dai giudici sovranazionali. Infine, alcune riflessioni sulla *ratio* sottesa alla reiterata scelta legislativa del citato doppio binario e la prospettazione di una via d'uscita dalla problematica: la riconduzione di entrambe le categorie di illeciti ad un unico sistema punitivo, con applicazione del principio di specialità ex art. 9, l. 689/1981.

El artículo analiza el sistema de sanciones previsto en la legislación vigente en materia de privacidad, recientemente objeto de importantes modificaciones a nivel tanto comunitario como nacional. En el contexto de una concisa reconstrucción de los ilícitos administrativos y penales actualmente previstos por el GDPR y por el "Código de la Privacidad", se evidencian las cuestiones críticas relacionadas con la formulación de tales ilícitos. El legislador pareciera haber adoptado un sistema sancionatorio de doble vía: por tanto, la segunda parte del trabajo se dedica a evaluar la compatibilidad de este enfoque con el principio *ne bis in idem*, conforme los lineamientos que han desarrollado los tribunales supranacionales. Por último, se efectúan algunas reflexiones sobre la lógica que subyace a la elección legislativa de establecer un sistema sancionatorio de doble vía y eventuales perspectivas de solución del problema: la reconducción de ambas categorías de delitos a un único sistema sancionador, con aplicación del principio de especialidad, de conformidad con el artículo 9 de la Ley 689/1981.

The paper aims to analyse the sanctioning system for privacy-related infringements, as recently amended both at the EU and the domestic level. Considering the administrative and criminal provisions currently provided for by the GDPR and the Italian Privacy Code, some critical issues will be highlighted with respect to the wording of the said provisions, whose interpretation is often difficult. The Italian lawmaker seems to have adopted the 'double track' sanctioning system: in the second part of the paper will assess the compatibility of the said system with the supranational principle of ne bis in idem. Finally, some reflections will be devoted to the rationale of the repeated option for the 'double track' sanctioning system, trying to find a way out from it through the 'specialty' principle established under art. 9 of Law 689/1981.

Sommario

1. Premessa.

Il presente lavoro[1] ha ad oggetto l'analisi critico-ricostruttiva del nuovo apparato sanzionatorio previsto dalla vigente normativa in ambito privacy. Come noto, tale materia è stata recentemente oggetto di importanti modifiche, comunitarie prima e nazionali poi, che hanno portato ad un panorama normativo composito e complesso: alla l. 196/2003 (cd. Codice Privacy, così come modificato dal d.lgs. 101/2018) si aggiungono il Regolamento UE 2016/679 (cd. GDPR) ed il settoriale d.lgs. 51/2018, attuativo della Direttiva UE 2016/680, in materia di trattamento dati per finalità di prevenzione e repressione di reati.

Quanto *infra* si prospetta deriva dalla difficoltà dell'intrico normativo della descritta disciplina, con il tentativo di far luce su ciò che sia lecito aspettarsi dall'attuale novellato impianto sanzionatorio. L'obiettivo non è quello di fornire risposte definitive ma piuttosto evidenziare gli aspetti più critici e prospettare soluzioni quanto più possibile verosimili. Come si vedrà, non sono pochi gli aspetti normativi che possono condurre (almeno) ad una duplice interpretazione. Per questo, l'analisi procederà per *step*: a seconda della risposta prospettata rispetto alla problematica evidenziata, potranno aprirsi ulteriori criticità alle quali, di nuovo, si cercherà di affiancare una possibile soluzione.

Punto focale dell'intero lavoro è la valutazione sulla sussistenza o meno di un doppio binario sanzionatorio tra illeciti amministrativi e penali. In altre parole, il legislatore ha previsto – come già fatto in altri campi, si pensi agli illeciti tributari o finanziari – una doppia risposta sanzionatoria per medesime violazioni? Ovvero opera la regola generale di cui all'art. 9, l. 689/1981, che prevede il principio di specialità scongiurando così un cumulo di sanzioni? Il doppio binario sanzionatorio, come noto, non è ad oggi censurato *tout court*, né a livello nazionale né sovranazionale, a condizione che rispetti determinati requisiti elaborati in tempi piuttosto recenti in seno alle Corti di Strasburgo e Lussemburgo. Ammesso che una doppia risposta sanzionatoria amministrativo-penale sussista, in questa sede si passerà infine a 'setacciare' la disciplina punitiva attraverso le maglie di detti requisiti di matrice giurisprudenziale che, se e solo se rispettati, legittimano il doppio binario.

2. Gli illeciti amministrativi.

Il catalogo e i criteri di determinazione delle sanzioni amministrative[2] sono, oggi, direttamente previsti all'art. 83 del Regolamento UE 2016/679, l'ormai ben noto GDPR. Mentre al paragrafo 2 dell'articolo sono elencati i criteri cui l'Autorità amministrativa deve fare riferimento ai fini della determinazione in concreto della sanzione da infliggere, i paragrafi 5 e 6 della norma prevedono le due distinte categorie di violazioni alle quali corrispondono sanzioni di diversa entità: per gli illeciti meno gravi è prevista una pena pecuniaria fino a 10 milioni di euro e, per le persone giuridiche, fino al 2% del fatturato mondiale annuo, qualora sia superiore alla somma anzidetta; pene più severe, invece, per le violazioni più gravi: fino a 20 milioni di euro per la persona fisica, ovvero al 4% del fatturato mondiale annuo per l'ente, se superiore[3].

La norma va, inoltre, letta in combinato disposto con l'art. 166 del Codice Privacy – unica norma sopravvissuta al d.lgs. 101/2018, che ha abrogato quasi *in toto* il capo I, rubricato "Violazioni Amministrative", in un'ottica di adeguamento al testo del GDPR –, che indica le

[1] È doveroso, anzitutto, un sentito ringraziamento alla prof.ssa Alessandra Rossi, che ha saputo dare un contributo fondamentale alle riflessioni oggetto del presente lavoro, in particolare nell'ambito del rapporto tra *ne bis in idem* e principi costituzionali.
[2] Per un maggior approfondimento sull'apparato sanzionatorio amministrativo v., *ex multis*, Bistolfi e Bolognini (2016); Ratti (2017); Cottu (2018); Del Ninno (2018a).
[3] Cfr. sull'argomento Marini (2017).

diverse norme interne allo stesso Codice Privacy le cui violazioni sono sottoposte alle pene pecuniarie appena descritte. Ai fini del presente lavoro e dell'analisi del doppio binario sanzionatorio interessano, in particolare, quelle condotte che siano comuni ad illeciti amministrativi e penali, vale a dire: violazioni in tema di servizi di comunicazione elettronica (artt. 123, 126, 129 e 130: trattamento dei dati relativi al traffico o all'ubicazione degli utenti; prescrizioni imposte dal Garante sulle modalità di inserimento ed uso dei dati personali degli utenti presenti in elenchi pubblici, cartacei e/o elettronici; uso dei dati per finalità di *marketing* telematico); violazioni concernenti il trattamento, per motivi di interesse pubblico rilevante, di categorie particolari di dati personali (art. 2 *sexies*), ovvero riguardanti misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute (art. 2 *septies*); oppure, ancora, violazioni nell'ambito del trattamento di dati relativi a condanne penali, misure di sicurezza e reati (art. 2 *octies*).

3. Gli illeciti penali.

Le fattispecie delittuose sono previste al Capo II del Titolo III del Codice Privacy, in particolare dall'art. 167 all'art. 172. Il d.lgs. 101/2018 ha in sostanza confermato l'impianto sanzionatorio esistente, aggiungendo tre nuove ipotesi di reato[4] ed abrogandone una soltanto[5].

Ai fini della presente ricerca, è utile e sufficiente focalizzare l'attenzione su una sola fattispecie, vale a dire il 'trattamento illecito di dati' previsto e punito dall'art. 167 Cod. Privacy, permettendoci di rinviare all'allegato normativo per la lettura integrale delle altre ipotesi di reato[6].

La norma, nell'ipotesi base di cui al primo comma, prevede la pena della reclusione da sei a diciotto mesi per 'chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli artt. 123, 126 e 130 o dal provvedimento di cui all'art. 129, arreca nocumento all'interessato'.

Urge anzitutto evidenziare la clausola di salvaguardia in apertura di norma, che esclude l'applicabilità del reato quando il fatto costituisca più grave reato: qualora, ad esempio, l'illecito trattamento dei dati posto in essere integri la diversa e più grave fattispecie di diffamazione aggravata, allora dovrà escludersi il concorso tra reati, con applicazione esclusiva di quest'ultimo delitto.

Soggetto attivo del reato può essere 'chiunque' commetta una delle condotte indicate: nonostante l'ampia portata del pronome, l'agente potrà tuttavia essere esclusivamente il titolare o il responsabile del trattamento, ovvero un 'soggetto designato' al quale siano assegnati compiti e funzioni connessi al trattamento dei dati ai sensi dell'art. 2-*quaterdecies* Cod. Privacy; la persona offesa, invece, è individuata in via esclusiva nell'interessato, vale a dire la persona fisica titolare dei dati.

Oltre alla condotta in violazione delle prescrizioni citate, è richiesta altresì la realizzazione di un evento: il nocumento dell'interessato. Il passaggio da reato di mera condotta a reato di evento rappresenta un'importante novità normativa, con ricadute di non poco conto in tema di successione delle leggi penali nel tempo: in effetti, la nuova fattispecie contempla un elemento costitutivo ulteriore e si distingue, rispetto alla versione precedente, sotto il profilo della specialità per aggiunta, così realizzando una *abolitio criminis* parziale. La nuova norma, maggiormente restrittiva della responsabilità penale, andrà applicata retroattivamente e permetterà ai condannati in via definitiva di promuovere incidenti di esecuzione *ex* art. 673 c.p.p., fondati sulla richiamata *abolitio*. L'aspetto che più interessa in questa sede concerne, però, il peso che questa modifica ha avuto sull'esistenza del doppio binario sanzionatorio: si può parlare di una doppia reazione punitiva da parte dello Stato in funzione di un *idem factum*? Al tema verrà riservato ampio spazio nel prosieguo.

[4] Si tratta delle fattispecie di: comunicazione e diffusione illecita di dati oggetto di trattamento su larga scala (art. 167 *bis*), acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (art. 167 *ter*) e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante (art. 168, co. 2).

[5] Il d.lgs. 101/2018 ha eliminato la distinzione tra misure di sicurezza idonee e minime ed ha conseguentemente abrogato il reato di cui all'art. 169, rubricato 'misure di sicurezza', che puniva l'omessa adozione delle misure di sicurezza minime nel trattamento dei dati personali.

[6] Per una più approfondita disamina sull'apparato sanzionatorio penale in materia privacy: Manes e Mazzacuva (2019); D'Agostino (2019); Finocchiaro (2018); Del Ninno (2018b).

Quanto poi alle condotte penalmente rilevanti elencate all'art. 167 Cod. Privacy, queste coincidono con quelle contemplate dagli illeciti amministrativi di cui già s'è detto al paragrafo precedente: si tratta, come visto, di violazioni delle prescrizioni di cui agli artt. 123, 126, 130 e di quanto previsto dal provvedimento del Garante di cui all'art. 129, in materia di inserimento ed uso di dati personali in elenchi pubblici.

Decisamente particolare è poi il delineamento dell'elemento soggettivo richiesto per la configurabilità del reato. Siamo al cospetto, evidentemente, di un dolo specifico: il legislatore richiede infatti che il soggetto abbia agito al fine di trarre profitto per sé o per altri ovvero – e questa sì che rappresenta quantomeno una peculiarità nel nostrano ordinamento penale – per arrecare danno all'interessato. Posto che la nozione di nocumento può essere intesa in senso più ampio rispetto a quella di danno – andando a comprendere qualunque pregiudizio, patrimoniale o non patrimoniale –, ecco che, qualora il motivo che muove l'agente sia quello di arrecare danno alla persona offesa, il fine specifico ben può finire per coincidere con l'evento, quando questo consista in un danno patrimoniale, in sostanza annullando l'elemento caratterizzante di tal categoria di dolo.

Veniamo ora ai commi secondo e terzo dell'art. 167, che prevedono un'ipotesi di reato aggravata, con pena della reclusione da uno a tre anni, quando oggetto della violazione siano prescrizioni in materia di dati caratterizzati da maggior delicatezza. In particolare, il primo capoverso punisce il trattamento di dati sensibilissimi, indicati agli artt. 9 e 10 GDPR – rilevatori, rispettivamente, dell'origine razziale, etnica, dell'ideologia politica, del credo religioso, dell'orientamento sessuale, dell'appartenenza sindacale o ancora dati genetici, biometrici, o sullo stato di salute del soggetto oppure, infine, concernenti reati, condanne o misure di sicurezza in ambito penale –, qualora avvenga in violazione delle prescrizioni di cui agli artt. 2 *sexies*, 2 *septies*, 2 *octies* o 2 *quinquiesdecies*. Il secondo capoverso, invece, punisce il trasferimento di dati personali verso un Paese terzo ovvero una organizzazione internazionale, fuori dai casi consentiti dagli artt. 45, 46 e 49 del GDPR: in breve, è necessario che il Paese o l'ente destinatario dei dati assicuri un livello sufficiente di protezione degli stessi, requisito questo previamente sottoposto al vaglio della Commissione europea; in mancanza di tal presupposto, i dati possono essere trasferiti all'estero solo qualora il titolare o il responsabile del trattamento offrano idonee garanzie e sempre che gli interessati possano disporre di diritti azionabili e mezzi di ricorso effettivi. L'art. 49 GDPR elenca ulteriori requisiti che, in assenza delle condizioni appena viste, rendono comunque lecita 'l'esportazione' dei dati: tra questi, il consenso dell'interessato, la necessità di trasferimento per l'esecuzione di un contratto in favore dell'interessato o del quale questi sia parte o, ancora, qualora ciò sia necessario nell'ambito di una vicenda giudiziaria nella quale l'interessato sia coinvolto. Infine, entrambe le aggravanti condividono con l'ipotesi base la clausola di esclusione in apertura – tipica, normalmente, di fattispecie autonome piuttosto che di ipotesi aggravate –, la necessaria realizzazione di un nocumento all'interessato e l'elemento soggettivo del dolo specifico.

4. Doppio binario sanzionatorio *versus* unico binario sanzionatorio.

Così presentate le linee generali dell'apparato sanzionatorio amministrativo e penale che legislatore europeo e italiano, in concorso, hanno confezionato, veniamo al momento essenziale del lavoro e domandiamoci: in occasione di un'unica condotta, è prevista una doppia risposta punitiva? In altre parole: qualora l'unico fatto posto in essere dall'agente integri al contempo un illecito amministrativo ed un illecito penale, egli dovrà attendersi un doppio procedimento ed una doppia punizione?

La norma da analizzare al fine di comprendere il rapporto tra sfera amministrativa e penale è l'art. 167 Cod. Privacy, nella parte che, in questa sede, non è stata ancora commentata, vale a dire i commi 4, 5 e 6, che regolano aspetti procedurali della disciplina.

Il quarto comma prevede che 'il Pubblico Ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante'. In questo caso, la disposizione ben permette di immaginare un parallelismo tra procedimento penale e procedimento amministrativo, il primo instaurato per iniziativa del Pubblico Ministero, il secondo dal Garante su segnalazione della pubblica accusa.

Il comma quinto dispone invece che il Garante trasmette al PM, con una relazione motivata, la documentazione raccolta durante l'attività di accertamento nel caso in cui emergano elementi che facciano presumere l'esistenza di un reato; ciò deve avvenire al più tardi entro la fine dell'attività di accertamento di violazioni amministrative previste dal Codice privacy. Ecco che il corrispettivo obbligo di cooperazione previsto in capo al Garante è formulato in maniera decisamente più articolata: il legislatore non si è limitato a riprendere la stessa formula utilizzata al comma precedente semplicemente invertendone i soggetti attivi, ma ha specificato che l'Autorità Amministrativa non solo deve dare notizia, ma deve procedere alla trasmissione della documentazione raccolta, accompagnandola con una relazione motivata. La norma non si preoccupa invece di indicare quali siano le fattispecie di reato in presenza delle quali scatti tale obbligo, come invece accade per il Pubblico Ministero: la trasmissione deve avvenire tutte le volte in cui il Garante prospetta la sussistenza di un qualsiasi fatto di reato, oltre all'illecito amministrativo, ovvero solo in relazione ad illeciti penali in materia privacy? Ad esempio, qualora il Garante individui i profili di una diffamazione, dovrà darne comunicazione, nelle forme viste, all'Autorità Giudiziaria? Il punto non è chiaro. Il necessario accompagnamento della segnalazione con la relazione motivata sembrerebbe limitare l'attività del Garante agli illeciti di cui abbia una più approfondita conoscenza e relativamente ai quali abbia svolto o stia svolgendo attività di accertamento; d'altra parte, la mancata indicazione dei reati per i quali sia richiesta siffatta trasmissione – prevista, come visto, per il Pubblico Ministero – potrebbe indicare una volontà legislativa nel senso di un'applicazione estensiva e generica della norma.

Ancora il comma in commento offre un ulteriore interessante spunto di riflessione: il termine entro il quale il Garante deve trasmettere la documentazione coincide con la fine dell'attività di accertamento. Assumendo che l'obbligo di trasmissione sussista esclusivamente per reati in materia di privacy – punto sul quale, come detto, la formulazione normativa non può dirsi cristallina –, cosa ne è del procedimento amministrativo? È destinato ad interrompersi in nome del principio di specialità *ex* art. 9, l. 689/1981, ovvero procede parallelamente all'azione penale? Il dubbio è lecito: negli altri ambiti in cui il legislatore italiano ha previsto la disciplina del doppio binario sanzionatorio, in effetti, la deroga al principio di specialità appena menzionato è espressa. A titolo esemplificativo, gli illeciti amministrativi previsti agli artt. 187 *bis* e *ter* del d.lgs. 58/1998 (Testo Unico della Finanza, T.U.F.) – che descrivono condotte del tutto sovrapponibili a quelle punite dai delitti di abuso di informazioni privilegiate e manipolazione di mercato – esordiscono con la clausola inclusiva 'salve le sanzioni penali quando il fatto costituisce reato'.

Chi scrive propende per la seconda soluzione prospettata, anche e soprattutto sulla base di quanto disposto dall'ultimo comma dell'art. 167 Cod. Privacy. Per quanto non sia presente una deroga esplicita al principio di specialità, la disposizione prevede che 'quando per lo *stesso fatto* è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita': il legislatore assume, evidentemente, che un procedimento amministrativo sia iniziato e terminato con l'inflizione di una sanzione, nonostante lo *stesso fatto* abbia permesso altresì di incardinare un procedimento penale. Proprio il comma sesto contiene il più 'grave' indizio nel senso della sussistenza del doppio binario sanzionatorio, che permette di affermare che è il legislatore stesso ad ammettere che in funzione del medesimo fatto il soggetto possa essere punito amministrativamente e penalmente. Ci limitiamo, per il momento, a sottolineare tale aspetto, rinviando al par. 6 il commento sulle evidenti criticità che tale disposizione – pur preziosa ai fini dell'individuazione della duplice risposta sanzionatoria – presenta.

Doppio binario sì, dunque. È possibile, a questo punto, procedere a valutare la liceità della duplice risposta sanzionatoria alla luce dei criteri elaborati dalla giurisprudenza sovranazionale – riassunti, per comodità del lettore, nel paragrafo che segue –, fondamentali ai fini della compatibilità della disciplina in commento con il principio del *ne bis in idem*.

5. I criteri di compatibilità di doppio binario sanzionatorio e *ne bis in idem*.

"*In the future, everyone will be world-famous for fifteen minutes*", diceva Andy Warhol. La questione del *ne bis in idem* supera la profezia, giocando un ruolo da grande protagonista nel

dibattito dottrinale e giurisprudenziale da almeno un quinquennio.

Linfa vitale alla tematica – soprattutto in Italia, in particolare a Torino – arrivò nel marzo 2014 dalla arcinota sentenza cd. Grande Stevens[7], con cui la Corte Europea dei Diritti dell'Uomo (da ora in avanti Corte EDU) condannò l'Italia per aver violato il divieto di doppio giudizio sancito all'art. 4 del prot. 7 CEDU. In breve, i ricorrenti lamentarono di essere stati ingiustamente sottoposti ad un doppio giudizio con conseguente violazione del principio *ne bis in idem*: a fronte di una condanna al pagamento di una severa sanzione pecuniaria per l'illecito amministrativo di cui all'art. 187 *ter* T.U.F., i ricorrenti furono imputati e processati, in funzione della medesima condotta, per la fattispecie di cui all'art. 185 T.U.F.

La Corte, come accennato, condannò l'Italia, dichiarando l'impossibilità di iniziare o proseguire un procedimento (penale o amministrativo), per uno stesso fatto e nei confronti di un medesimo soggetto, qualora lo stesso sia già stato giudicato in via definitiva al termine di altro procedimento (di nuovo, penale o amministrativo).

Tra i passaggi fondamentali della sentenza rientra certamente l'individuazione, da parte dei giudici di Strasburgo, di tre fondamentali elementi, necessari al fine di valutare l'esistenza di una situazione in contrasto con il *ne bis in idem*.

Anzitutto, deve valutarsi la natura giuridica delle sanzioni inflitte, delineando sotto il profilo sostanziale e non meramente nominale il confine della *matiére pénale*: ed in effetti, il divieto di doppio giudizio così come convenzionalmente disciplinato al già citato art. 4, prot. 7, CEDU, impedisce la duplicazione dei giudizi esclusivamente nell'ambito penale[8]. Nella pronuncia citata, la Corte riprende i tre cd. criteri Engel, elaborati in un'altra nota sentenza emessa da Strasburgo del lontano 1976[9]: non basterà all'interprete guardare alla denominazione data dal legislatore alla sanzione – che, nel nostro caso, rimanda nominalmente alla sfera amministrativa –, ma dovrà altresì badare alla finalità e alla gravità della stessa. I giudici, considerata la severità delle sanzioni pecuniarie previste dall'art. 187 *ter* – da euro ventimila a cinque milioni, triplicabili qualora appaiano inadeguate – e, conseguentemente, l'evidente finalità afflittivo-retributiva delle stesse, tipica della sfera penale, hanno ritenuto che l'illecito amministrativo fosse da considerarsi 'sostanzialmente penale'. In secondo luogo – e questo è uno dei punti più caldi nell'economia del presente lavoro – dovrà accertarsi l'unicità e la medesimezza del fatto contestato, sul quale si fonda il doppio giudizio. Anche in questo caso, la Corte si allontana dall'impostazione formale e lascia il passo alla sostanza, rifiutando l'*idem* legale in favore dell'*idem factum*[10]. Il discorso verrà ripreso ed approfondito nei paragrafi seguenti, per il momento è sufficiente tenere a mente che l'interprete non dovrà guardare alla diversa qualificazione normativa data dal legislatore ad una medesima condotta, ma dovrà limitarsi a considerare il fatto, così come posto in essere, nella sua realizzazione storico-naturalistica. Proprio questa parte della sentenza ha poi dato luogo alla declaratoria di parziale illegittimità costituzionale dell'art. 649 c.p.p.[11], disciplinante il divieto di *bis in idem* processuale, nella parte in cui escludeva la medesimezza della condotta in caso di concorso formale di reati *ex* art. 81 c.p. Sì tornerà sul punto. Infine, la terza e ultima valutazione del giudice per accertare la sussistenza di un *bis in idem* concerne l'effettiva duplicità di giudizio, presente solo quando il provvedimento emanato per primo sia già divenuto definitivo e vi sia identità soggettiva tra i destinatari.

La strada intrapresa dalla 'sentenza Grande Stevens' di condanna *in toto* dei meccanismi di doppio binario sanzionatorio, sancita dal divieto di iniziare o proseguire un nuovo giudizio sull'*idem factum* in presenza di un giudicato 'sostanzialmente penale', subisce un'importante battuta d'arresto nel novembre del 2016. Con la sentenza A e B c. Norvegia[12] – concernente una supposta violazione, da parte dello disciplina norvegese in materia tributaria, del divieto di *bis in idem* – la Corte EDU conferma gli approdi della sentenza appena commentata, ma lancia un'àncora di salvezza per il doppio binario: è fatto divieto di iniziare o proseguire un nuovo

[7] Sent. Corte EDU, 4 Marzo 2014, Grande Stevens e altri c. Italia.
Tra i numerosi commenti alla pronuncia si segnalano: Viganò (2016a); Fidelbo (2014a e b).
[8] Art. 4, prot. 7, CEDU: 'Nessuno potrà essere perseguito o condannato penalmente dalla giurisdizione dello stesso Stato per un'infrazione per cui è già stato scagionato o condannato a seguito di una sentenza definitiva conforme alla legge ed alla procedura penale di tale Stato'.
[9] Sent. Corte EDU, 23 novembre 1976, Engel e altri c. Paesi Bassi
[10] Tale nozione di *idem factum* è stata ripresa dalla Corte di Strasburgo da una precedente e fondamentale pronuncia della stessa Corte, vale a dire sent. Corte EDU (Grande Chambre), 10 febbraio 2009, Zolotukhin v. Russia
[11] Sent. C. Cost., 21 luglio 2016, n. 200.
[12] Sent. Corte EDU (Grande Chambre), 15 novembre 2016, A e B c. Norvegia.
Si segnalano, *ex multis*, i seguenti commenti alla pronuncia: Fimiani (2017); Viganò (2016b).

giudizio per un medesimo fatto nei confronti di una medesima persona, a meno che tra i due procedimenti sussista una '*sufficiently close connection in substance and time*'. L'espressione, ormai nota, sin dall'inizio non parve brillare per chiarezza e la giurisprudenza si sforzò di elaborare criteri valutativi maggiormente precisi[13], che riportiamo qui di seguito: i due apparati sanzionatori devono perseguire scopi differenti e concernere aspetti diversi della medesima condotta; la doppia punibilità deve essere prevedibile; le due autorità titolari dei procedimenti devono agire con modalità integrate, al fine di evitare il più possibile ogni ripetizione nella raccolta e nell'esperimento degli elementi probatori; ancora – ed è verosimilmente questo il criterio più importante –, la sanzione irrogata per prima deve essere tenuta in debito conto nella determinazione del *quantum* della seconda sanzione inflitta. Infine, per quanto non sia necessario che i procedimenti procedano parallelamente per tutta la loro durata, il cumulo temporale dei due non può e non deve bloccare l'individuo in una situazione di 'perdurante incertezza'.

Se è vero che la Corte di Strasburgo si è per prima interessata al *ne bis in idem*, anche la Corte di Giustizia dell'Unione Europea si è spesa nella tematica in oggetto. Il divieto del doppio giudizio in materia penale è tutelato all'art. 50 della Carta di Nizza, rubricato 'diritto di non essere giudicato o punito due volte per lo stesso reato', che prevede testualmente che 'nessuno può essere perseguito o condannato per un reato per il quale è già stato assolto o condannato nell'Unione a seguito di una sentenza penale definitiva conformemente alla legge'. Del pari, la giurisprudenza comunitaria riprende la citata *sufficiently close connection in substance and time*, declinando i criteri valutativi che il giudice nazionale deve considerare per accertare l'eventuale violazione del *ne bis in idem* in maniera non dissimile da quanto già fatto nella citata sentenza 'A e B c. Norvegia'[14]. I due procedimenti devono perseguire finalità diverse e prevedere meccanismi di coordinamento finalizzati a ridurre al minimo gli oneri connessi al reperimento e all'accertamento probatorio; gli illeciti devono punire aspetti complementari del medesimo comportamento illecito; inoltre, la doppia risposta punitiva deve essere prevedibile e il cumulo delle due sanzioni deve rispettare il principio di proporzionalità. Infine, anche i giudici di Lussemburgo richiedono un collegamento di natura cronologica tra i procedimenti[15].

6. *Focus*: la nozione di *idem factum* convenzionale ed italiana a confronto.

Prima di procedere alla valutazione della compatibilità del descritto impianto sanzionatorio con i criteri sinora evidenziati, ancora una necessaria precisazione, fondamentale ai fini del prosieguo del lavoro, concernente la nozione di *idem factum* così come recepita dalla giurisprudenza nostrana.

Come noto, sul punto si è espressa la Corte Costituzionale con la sent. 200/2016[16]. La questione di legittimità costituzionale fu sollevata dal Giudice dell'Udienza Preliminare del Tribunale di Torino in seno al secondo procedimento incardinato a carico di colui che, all'epoca dei fatti contestati, era amministratore della società Eternit. A seguito del proscioglimento per estinzione del reato per intervenuta prescrizione – nel cd. processo Eternit I si contestava i reati di disastro innominato e di omissione dolosa di cautele contro gli infortuni sul lavoro, di cui agli artt. 434, co. 2, e 437, co. 2, c.p. –, la pubblica accusa aveva chiesto il rinvio a giudizio nei confronti dello stesso imputato e relativamente agli stessi fatti per omicidio colposo. Il GUP torinese dubitava della legittimità costituzionale dell'art. 649 c.p.p. in quanto incompatibile con il già menzionato art. 7, prot. IV, CEDU – così come interpretato alla luce della giurisprudenza di Strasburgo in materia di *idem factum*, citata in precedenza – per la diversa nozione italiana di medesimo fatto: la norma interna, secondo il giudice *a quo*, limitava tal concetto all'*idem* legale, escludendo il *bis in idem* qualora l'azione od omissione dell'agente fosse idonea ad integrare fattispecie di reato diversamente qualificate.

[13] Per una puntuale analisi della giurisprudenza europea e italiana sul punto si veda, tra gli altri, De Franceschi (2018).
[14] Il tema è stato affrontato in tre pronunce originate da rinvii pregiudiziali di giudici italiani, concernenti la compatibilità del doppio binario sanzionatorio in materia di reati tributari e di *market abuse* con l'art. 50 della Carta di Nizza, interpretato alla luce dell'art. 4, prot. 7, CEDU: Corte di Giustizia UE, Grande Sezione, 20 marzo 2018, C-524/15, Menci; C-537/16, Garlsson Real Estate e a.; C-596/16 e C-597/16, Di Puma e Zecca.
[15] Sul punto, Galluccio (2018).
[16] C. Cost., sent. del 21 luglio 2016, n. 200. Sul tema, tra gli altri, Pulitanò (2017); Viganò (2016c); Ferrua (2017).

La Consulta dichiara la parziale incostituzionalità dell'art. 649 c.p.p. '*nella parte in cui esclude che il fatto sia il medesimo per la sola circostanza che sussiste un concorso formale tra il reato già giudicato con sentenza divenuta irrevocabile e il reato per cui è iniziato il nuovo procedimento penale*'. Il cd. processo Eternit *bis*, tuttavia, non si arresta. La Corte, pur richiamando la giurisprudenza convenzionale e rifiutando la nozione di *idem* legale, annovera nella nozione di *idem factum* non solo la condotta, ma anche l'evento e il nesso causale (la cd. 'triade'), pur sempre considerati esclusivamente nella loro dimensione empirica. In altre parole, la Consulta nega che la Corte EDU abbia mai esplicitamente inteso restringere l'analisi alla sola condotta, escludendo dal *range* di valutazione gli altri due elementi appena detti: l'unico motivo per cui l'interpretazione convenzionale considera esclusivamente azione od omissione è da rinvenirsi nella natura degli illeciti oggetto delle pronunce, tutti di mera condotta. Sulla base di questa considerazione, la Corte 'salva' il processo Eternit *bis* dalla declaratoria di improcedibilità, permettendone la prosecuzione.

Tuttavia, il 'nodo' relativo a ciò che debba essere ricompreso nella nozione di *idem factum* non era stato univocamente sciolto nella sentenza della Corte EDU Zolotukhin c. Russia del febbraio 2009 – che, come accennato, inaugurò la 'nuova stagione' della nozione di medesimezza del fatto – e, nell'ottica di chi scrive, l'impostazione adottata dalla Consulta non è pienamente condivisibile: il riferimento alla 'triade' condotta-nesso causale-evento rischia, a ben vedere, di (ri)avvicinare pericolosamente l'*idem factum* all'*idem* legale, andando a ricomprendere un elemento di differenziazione che può essere solamente eventuale. L'unico momento che rientra nel pieno dominio del soggetto agente e che, necessariamente, si realizza è, in effetti, l'azione o l'omissione da questi posta in essere, mentre l'evento realizzatosi 'fuoriesce' giocoforza da questo *range*. Per meglio comprendere il presente ragionamento si pensi alla valutazione sulla medesimezza del fatto concernente un illecito amministrativo ed un delitto, qualora quest'ultimo si sia realizzato esclusivamente nella forma tentata: se davvero è necessario, secondo l'insegnamento della giurisprudenza convenzionale, attenersi all'accadimento storico-naturalistico, ponendosi nella prospettiva di un osservatore esterno, ecco che non potrà che parlarsi di *idem factum*, non sussistendo l'elemento differenziale dell'evento, né del nesso causale. Il solo profilo di distinzione ravvisabile sarebbe quello dell'elemento soggettivo che, però, certo non rientra nella valutazione concreta e fattuale di cui s'è detto in precedenza. Non rimane che domandarci se davvero si possa ritenere tollerabile una diversa valutazione dello stesso fatto – e la conseguente sottoposizione o meno dell'agente ad un doppio giudizio – fondata sulla sussistenza di un elemento, l'evento, posto fuori dalla sfera di controllo del soggetto agente e pesantemente influenzato da fattori causali terzi.

Tutto questo per dire che, verosimilmente, la giurisprudenza italiana escluderà l'ipotesi di *bis in idem* tra illecito penale ed amministrativo in ambito privacy, forte dell'elemento differenziale dell'evento che, lo ricordiamo, è contemplato nella fattispecie di reato ma non in quella amministrativa. Ciò tuttavia deriverebbe da un'impostazione non del tutto corretta e non completamente conforme al lascito della giurisprudenza sovranazionale.

7. Disciplina privacy e *ne bis in idem*: un bilancio riassuntivo.

Ammettendo, dunque, che l'attuale disciplina privacy contempli un doppio binario sanzionatorio penale-amministrativo e che l'elemento dell'evento, richiesto ai fini dell'integrazione della fattispecie delittuosa, non valga ad escludere l'*idem factum*, non resta che vagliarne la 'sufficiente connessione sostanziale e temporale' alla luce dei criteri elaborati tra Strasburgo e Lussemburgo, elencati *supra* (par. 4).

Se può certamente ritenersi rispettato il criterio della prevedibilità della doppia risposta punitiva prevista dal legislatore, appare invece difficile sostenere che i due impianti sanzionatori perseguano scopi differenti: la severità delle sanzioni amministrative – lo ricordiamo, l'art. 83 GDPR prevede sanzioni pecuniarie fino a 10.000 o 20.000 euro, a seconda della gravità della violazione, per le persone fisiche e fino al 2% o al 4% del fatturato mondiale annuo per gli enti – rimanda ad una finalità spiccatamente retributiva e punitiva, tipica e già contemplata dall'illecito penale.

Quanto al coordinamento tra procedimenti, i commi quarto e quinto dell'art. 167 Cod. Privacy –connotati, come visto, da un certo grado di incertezza interpretativa dettata da una formulazione non speculare degli obblighi di informazione spettanti all'autorità giudiziaria

ed amministrativa (v. *supra*, par. 3) – prevedono un dialogo biunivoco, in fase iniziale, tra il Garante e la pubblica accusa. Nulla tuttavia è previsto sotto il profilo della non dispersione probatoria.

Ardua impresa, poi, è vagliare astrattamente il rispetto del cd. criterio temporale, considerato che spetta al giudice valutare, caso per caso, se l'individuo sia stato esposto all'incertezza sulla propria sorte processuale per un tempo – ottenuto sommando la durata dei due giudizi, nella parte in cui non abbiano proceduto parallelamente – eccessivamente lungo.

Da ultimo, veniamo a trattare di quel che si ritiene il vero *punctum dolens* della disciplina di 'connessione', vale a dire la proporzionalità della pena. L'ultimo comma dell'art. 167 Cod. Privacy prevede una diminuzione di pena – sotto forma, parrebbe, di attenuante ad effetto comune – qualora al reo, per il medesimo fatto, sia già stata *applicata e riscossa* una sanzione amministrativa. La disposizione è formulata in maniera quantomeno peculiare, specie se si procede ad un paragone con norme che assolvono al medesimo scopo di 'coordinamento sanzionatorio', previste in altre parti dell'ordinamento. Si permetta un riferimento, ancora una volta, alla disciplina del *market abuse*: l'art. 187 *terdecies* T.U.F. dispone, parafrasando, che tanto il giudice penale quanto la CONSOB, in sede di determinazione della sanzione da infliggere, debbano tenere conto delle misure punitive già irrogate. La differenza immediatamente rilevabile è duplice: da un lato, entrambe le Autorità debbono considerare le sanzioni già inflitte nel procedimento conclusosi per primo e, dall'altro, è sufficiente che la sanzione sia stata *irrogata* al termine di un procedimento divenuto definitivo. In ambito privacy, invece, tale incombenza è prevista solamente a carico dell'Autorità Giudiziaria, così escludendo qualsiasi tipo di bilanciamento in tal senso qualora a terminare per primo sia il procedimento penale (ipotesi questa tutt'altro che lontana dalla realtà qualora, ad esempio, il processo venga definito con il rito alternativo del patteggiamento). Inoltre, l'attenuante potrà applicarsi esclusivamente una volta riscossa, ciò che subordina ad una mera eventualità fattuale – la sanzione amministrativa è, in ogni caso, *res judicata*! – il necessario coordinamento richiesto delle Corti sovranazionali ai fini della legittimità della doppia risposta sanzionatoria.

Alla luce di quanto detto, dunque, non sembra che l'impostazione attuale del sistema sanzionatorio privacy sia in grado di superare il *test* della più volte nominata *sufficiently close connection in substance and time*, a causa del mancato rispetto dei suddetti criteri[17].

8. Conclusioni.

La lunga e forse complessa analisi prospettata porta a concludere che il novellato impianto sanzionatorio privacy che pare muoversi, come visto, su un doppio binario penale-amministrativo, non possa, allo stato attuale, considerarsi compatibile con il principio del *ne bis in idem* convenzionale e comunitario, con conseguente riduzione a 'lettera morta' della raccomandazione contenuta al Considerando 149 del GDPR.

In coda al lavoro, un'ultima e più severa considerazione. La compatibilità del doppio binario con il divieto di doppio giudizio appare, ancora oggi, un argomento spinoso: se è vero che le Corti sovranazionali hanno elaborato diversi criteri valutativi, è anche vero che questi non brillano per puntualità e chiarezza, lasciando al giudice nazionale un'eccessiva discrezionalità; il rispetto del nebuloso criterio temporale, in particolare, non è accertabile se non all'esito dell'intero *iter* processuale, ciò che rappresenta un vero e proprio 'sgambetto' al principio di legalità *ex* art. 25 Cost., in termini di certezza e prevedibilità del diritto. E ancora, si ritiene qui possibile azzardare un ulteriore profilo di incompatibilità del doppio binario con i principi costituzionali che reggono l'ordinamento penale nostrano. Ed in effetti, anche qualora la disciplina rispetti la connessione sostanziale e temporale, rimane che il soggetto, per un fatto unico, subisce un doppio procedimento ed una doppia sanzione – dei limiti della 'compensazione', specie in materia privacy, già s'è detto –, duplicità questa verosimilmente avvertita come eccessiva, ingiusta; posto che la pena, ai sensi dell'art. 27, co. 3, Cost., deve necessariamente tendere alla rieducazione del condannato, è realisticamente possibile aspettarsi che una risposta sanzionatoria avvertita come ingiusta sia in grado di perseguire uno scopo rieducativo?

[17] Perplessità sovrapponibili sono state sollevate da Manes e Mazzacuva (2019): gli Autori sottolineano come manchi completamente una disposizione che regoli il coordinamento delle attività svolte dalle due autorità coinvolte, anche e soprattutto in tema di non dispersione probatoria.

Il motivo che spinge il legislatore ad insistere, nonostante il non breve elenco di criticità nel tempo evidenziate, sulla via del doppio binario sanzionatorio sembra quello di voler marchiare determinati illeciti con lo stigma che caratterizza la condanna penale, senza però rinunciare – considerate le lacune, in termini di certezza e celerità della pena, che oggi non mancano nel sistema giudiziario penale, ma che in alcuna maniera sono riconducibili alla volontà dell'imputato – all'inflizione di severe sanzioni in tempi più brevi e certi, obiettivo più agevolmente raggiungibile sul fronte amministrativo.

La via d'uscita da questa *empasse* necessariamente passa, da un lato, dal riconoscimento dell'appartenenza della sfera penale e di quella amministrativa ad un unico sistema sanzionatorio – convivenza questa di cui è prova il generale principio di specialità *ex* art. 9, l. 689/1981, vistosamente derogato dalla disciplina del doppio binario – e, dall'altro, dall'arretramento della risposta penale, nel senso di un recupero del ruolo di *extrema ratio*, disegnando così un'unica risposta sanzionatoria statale, graduata su una scala di crescente gravità, dall'amministrativo al penale.

Bibliografia

Bistolfi, Camilla e Bolognini, Luca (2016): "*Le sanzioni*", in Bolognini, Luca, Pelino, Enrico e Bistolfi, Camilla: *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali* (Milano, Giuffrè), pp. 685 ss.;

Cottu, Enrico (2018): "*L'impatto del Regolamento generale sulla protezione dei dati sul sistema punitivo a livello eurounitario e sovranazionale*", in Mantelero, Alessandro e Poletti, Dianora (eds.): *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna* (Pisa, Pisa University Press);

D'Agostino, Luca (2019): "*La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101*", *Archivio Penale Web*, 1;

De Franceschi, Paola (2018): "*Ne bis in idem* e reati tributari: nel dialogo tra Corti trionfa il criterio della *sufficiently close connection in substance and time*", *Giurisprudenza Penale Web*, 4;

Del Ninno, Alessandro (2018): "Il decreto legislativo 101/2018 di modifica e coordinamento del Codice della Privacy al GDPR: uno sguardo d'insieme sul nuovo quadro normativo nazionale sulla tutela dei dati personali", in www.dirittoegiustizia.it;

Del Ninno, Alessandro (2018): "Il nuovo impianto sanzionatorio penale del Codice della privacy coordinato al GDPR. Le principali novità in materia di reati privacy", www.dirittoegiustizia.it;

Ferrua, Paolo (2017): "La sentenza costituzionale sul caso Eternit: il *ne bis in idem* tra diritto vivente e diritto vigente", *Cassazione Penale*, 1, pp. 78-90;

Fidelbo, Giorgio (2014): "Considerazioni sul principio del *ne bis in idem* nella recente giurisprudenza europea: la sentenza 4 Marzo 2014, Grande Stevens e altri c. Italia", *Corte di Cassazione, Ufficio del Ruolo e del Massimario*;

Fidelbo, Giorgio (2014): "Il principio del *ne bis in idem* e la sentenza 'Grande Stevens': pronuncia europea e riflessi nazionali", www.dirittopenaleeuropeo.it;

Fimiani, Pasquale (2017): "*Market abuse* e doppio binario sanzionatorio dopo la sentenza della Corte EDU, Grande Camera, 15 Novembre 2016, A e B c. Norvegia", *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2, pp. 5-20;

Finocchiaro, Giusella (2018): "Lo schema di decreto legislativo sulla privacy", www.filodiritto.it;

Galluccio, Alessandra (2018), "La Grande Sezione della Corte di giustizia si pronuncia sulle attese questioni pregiudiziali in materia di *bis in idem*", *Diritto Penale Contemporaneo – Rivista Trimestrale*, 3, pp. 286-294;

Manes, Vittorio e Mazzacuva, Francesco (2019), "GDPR e nuove disposizioni penali del codice privacy", *Diritto penale e processo*, 2, pp. 167-171;

Marini, Paolo (2017): "Regolamento Privacy UE e violazioni: le novità dell'apparato sanzionatorio", *Quotidiano giuridico*;

Pulitanò, Domenico (2017): "La Corte Costituzionale sul *ne bis in idem*", *Cassazione Penale*, 1, pp. 70-77;

Ratti, Matilde (2017): "*Il regime sanzionatorio previsto dal Regolamento per l'illecito trattamento dei dati personali*", in Finocchiaro, Giusella (eds.): *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* (Bologna, Zanichelli), pp. 595 ss.;

Viganò, Francesco (2016): "*Ne bis in idem* e contrasto agli abusi di mercato: una sfida per il legislatore e i giudici italiani. Riflessioni *de lege lata* e *ferenda* sull'impatto della sentenza Grande Stevens nell'ordinamento italiano", *Diritto Penale Contemporaneo – Rivista Trimestrale*, 1, pp. 186-202;

Viganò, Francesco (2016): "La grande camera della corte di Strasburgo su *ne bis in idem* e doppio binario sanzionatorio", www.penalecontemporaneo.it;

Viganò, Francesco (2016): "*Ne bis in idem* e doppio binario sanzionatorio in materia di abusi di mercato: dalla sentenza della Consulta un *assist* ai giudici comuni", www.penalecontemporaneo.it

Eternal Sunshine of the Spotless Crime. Informazione e oblio nell'epoca dei processi su internet

Eternal Sunshine of the Spotless Crime. *Información y olvido en la época de los procesos de internet*

Eternal Sunshine of the Spotless Crime. *The Right to Information and the Right to be Forgotten in Times of Trials by Media*

Edoardo Mazzanti
Assegnista di ricerca in Diritto Penale presso l'Università di Macerata
edoardo.mazzanti@unimc.it

Libertà di espressione, Diffamazione
Libertad de expresión, Difamación
Freedom of expression, Defamation

Abstracts

Processo penale e c.d. processo mediatico si differenziano, fra le altre, in ragione del diverso peso attribuito al fattore temporale: mentre il primo si sviluppa in senso diacronico, il secondo presenta natura pressoché istantanea, spesso esaurendosi nelle primissime fasi del procedimento vero e proprio. La divaricazione tra i due fenomeni si fa ancora più consistente laddove il canale mediatico sia internet, ove l'istantaneità del 'processo' si combina con la memorizzazione a oltranza del dato. Appare evidente, così, che eventuali articoli aventi a oggetto passate vicende criminali, se non rimossi, rettificati o semplicemente aggiornati, rischino di segnare irreversibilmente la dignità del soggetto coinvolto. Muovendo da tali acquisizioni, il presente lavoro si propone di indagare portata, pregi e limiti del c.d. diritto all'oblio nel peculiare contesto della cronaca giudiziaria via *web*.

Proceso penal y proceso mediático se diferencian, entre otras cosas, en razón del diverso peso atribuido al factor temporal: mientras el primero se desarrolla en sentido diacrónico, el segundo presenta una naturaleza casi instantánea, a menudo acabándose en las primeras etapas del procedimiento real. La brecha entre los dos fenómenos se vuelve aún más notoria cuando el medio de comunicación es internet, donde la instantaneidad del "proceso" se combina con la memorización hasta el amargo final de los datos. Aparece evidente, por tanto, que cualquier artículo relacionado con eventos criminales pasados, si no se elimina, rectifica o actualiza, corre el riesgo de marcar irreversiblemente la dignidad del sujeto involucrado. A partir de estas consideraciones, el presente trabajo tiene como objetivo investigar el alcance, los méritos y los límites del denominado "derecho al olvido", en el especifico contexto de las noticias judiciales en internet.

The passing of time has different relevance whether we deal with due process of law or 'trials by media': whereas the former develops over time, the latter has a basically momentary nature, considering that mass media tend to focus exclusively on criminal trials' very first steps. This divergence increases on the internet, where the 'judicial' immediacy meets all-time data storage. Thus, it is clear that, as time runs, old criminal convinction-related articles, where not erased, corrected or simply updated, may end up infringing the defendant's personal dignity. Moving from this framework, this paper aims at analyzing extent, virtues and limits of the 'right to be forgotten' in the peculiar context of criminal web-news.

Sommario

«E allora l'uomo dice 'mi ricordo' e invidia l'animale
che subito dimentica e che vede veramente morire,
sprofondare nella nebbia e nella notte, spegnersi
per sempre ogni istante.»
(F. NIETZSCHE, Sull'utilità e il danno della storia per la vita)

1. Introduzione.

Il diritto penale intrattiene un rapporto poliedrico col fattore tempo[1]. In linea generale, l'adeguamento della sanzione alle cadenze temporali della vita umana è in linea con una concezione non autoritaria del diritto penale, ispirata a esigenze di proporzione «non semplicemente rispetto al reato commesso, ma rispetto ai bisogni di risposta che il corso del tempo può ragionevolmente concorrere a modellare e ridurre, fino ad azzerare»[2]. Strettamente affiliate a istanze di tutela della personalità, tali esigenze di proporzione, nell'attuale temperie criminale, possono essere declinate in vario modo[3].

L'istituto che, più d'ogni altro, mira a regolare i rapporti tra decorso del tempo e responsabilità penale è fuor di dubbio la prescrizione. Senza poter indugiare su un tema tanto intricato quanto rovente, in questa sede è sufficiente rammentare che, fra le *rationes* tradizionalmente dedotte a fondamento della prescrizione, figura il diritto individuale all'oblio, oggetto di frequenti richiami anche nella recente giurisprudenza costituzionale[4]. Implicando la temporaneità dello *ius puniendi*, il diritto all'oblio assume, qui, una precisa connotazione personalistica, che pone un limite alla compressione delle aspettative individuali sancite in Costituzione e impedisce l'indefinita subordinazione del singolo alla pretesa statuale[5]. Breve: all'interno delle dinamiche penalistiche temporali, l'oblio si erge, al contempo, a garanzia dell'individuo e ad argine del potere punitivo.

Sennonché, l'erompere delle nuove tecnologie - e segnatamente, di internet - ha stravolto la concezione del fluire del tempo[6], svelandone, in ottica giuridica, la «preoccupante fragilità predicativa»[7]. Ciò rende i rapporti fra sistema penale e oblio suscettibili di nuove, interessanti declinazioni. Se ne segnalano, in particolare, due; trasposizioni - con buon grado d'approssimazione - di altrettante 'anime' che, nella sua tortuosa evoluzione, il diritto all'oblio medesimo ha assunto[8].

Secondo una prospettiva essenzialmente ancorata alla dimensione della riservatezza, nel diritto all'oblio è possibile ravvisare il contrappeso dell'interesse collettivo all'accertamento e

[1] Per una tematizzazione, Falcinelli (2011), pp. 1ss, 88ss.
[2] Pulitanò (2017), p. 244.
[3] Mostra alcune affinità rispetto alla tutela (*dal* diritto) penale *nel* tempo il divieto di *bis in idem*, che, mettendo al riparo il consociato dalle tentacolari proiezioni del potere punitivo, impedisce che «*il contatto con l'apparato repressivo dello Stato, potenzialmente continuo, [proietti] l'ombra della precarietà nel godimento delle libertà connesse allo sviluppo della personalità individuale*» (Corte cost., n. 200/2016, § 6 del *considerato in diritto*).
[4] Corte cost., n. 23/2013 (§ 3.1 del *considerato in diritto*); Corte cost., n. 143/2014 (§ 3 del *considerato in diritto*); Corte cost., n. 42/2015 (§ 6.3 del *considerato in diritto*); Corte cost., n. 257/2017 (§ 5 del *considerato in diritto*); Corte cost., n. 112/2018 (§ 4 del *considerato in diritto*).
[5] Giunta e Micheletti (2003), pp. 45ss.
[6] Scrive Castells (2002), p. 495: con l'avvento della rete, l'idea di tempo «lineare, irreversibile, misurabile, prevedibile sta andando in frantumi […] secondo un movimento di straordinario significato storico. Ma non stiamo assistendo solo a una relativizzazione del tempo in base ai contesti sociali o, in alternativa, al ritorno della reversibilità del tempo, come se la realtà potesse essere interamente catturata da miti ciclici. La trasformazione è più profonda: si tratta di rimescolare i tempi per creare un universo infinito, che non si autoespande ma si autoconserva, non ciclico ma casuale, non ricorsivo ma incursivo: un tempo senza tempo che usa la tecnologia per sfuggire ai contesti della sua esistenza e per appropriarsi in modo selettivo di qualsiasi valore ciascun contesto possa offrire al sempre-presente».
[7] Piergallini (2014), p. 2375.
[8] Un accurato inquadramento del diritto all'oblio nella congerie dei 'diritti alla personalità' è offerto da Bonavita (2016), pp. 50ss, il quale

alla prevenzione dei reati[9]. Si considerino, in proposito, le vicende in materia di *data retention*[10] e, prima su tutte, la cruciale sentenza *Digital Rights Ireland*[11]: nel giudicare la Dir. 2006/24/CE incompatibile coi limiti imposti dalla Carta dei Diritti Fondamentali dell'Unione Europea (d'ora in avanti, CDFUE), la Corte di Giustizia censurava, fra le altre, la fissazione di un termine di conservazione minimo effettuata senza distinzione alcuna fra le varie categorie di dati (§ 63) nonché l'assenza di criteri obiettivi in grado di limitare la conservazione al tempo strettamente necessario (§ 64). Nella complessa opera di contemperamento tra esigenze collettive ed esigenze del singolo, emerge, dunque, la chiara rilevanza del fattore temporale[12]; rilevanza, è appena il caso di accennarlo, scarsamente avvertita nel nostro ordinamento, che, complici i recenti innesti per mano della l. 167/2017[13] e del d.lgs. 101/2018[14], pare collocarsi ampiamente al di fuori del perimetro tracciato dalla Corte di Giustizia[15].

Ma il diritto all'oblio può presentare anche un volto diverso, più innovativo, prossimo al diritto all'identità personale[16] quale situazione giuridica tesa a proteggere la «*proiezione sociale della personalità dell'individuo, cui si correla un interesse del soggetto ad essere rappresentato, nella vita di relazione, con la sua vera identità*»[17]. Calato in quest'accezione sul terreno penalistico, l'oblio assurge a naturale contraltare della libertà di manifestazione del pensiero, *sub specie*, in particolare, del diritto di cronaca giudiziaria: è del tutto evidente, infatti, che la permanenza in rete di notizie relative a coinvolgimenti penali (veri o presunti, confermati o smentiti), a lungo andare, rischia di collidere col diritto fondamentale del singolo a vedersi rappresentato in modo storicamente contestualizzato.

Il presente contributo intende approfondire quest'ultimo aspetto. A tal fine, nelle pagine che seguono, chiariti brevemente i rapporti tra processo penale e c.d. processo mediatico con specifico riferimento al profilo temporale (§ 2), ci proponiamo di offrire, sia pur in modo stilizzato, un inquadramento del diritto all'oblio, scandagliandone le ragioni di fondo e ripercorrendone la recente evoluzione normativo-giurisprudenziale (§ 3). Successivamente, tenteremo di delineare la sagoma della c.d. vittima mediatica, soffermandoci sui beni che la disponibilità a oltranza di informazioni 'colpevoliste' rischia di pregiudicare (§ 4). Seguirà l'individuazione degli strumenti e delle sedi ove poter esercitare suddetto diritto (§ 5). In sede conclusiva, daremo conto delle importanti sfide che il rapporto diritto penale *versus* libertà d'informazione prospetta nell'epoca di internet (§ 6). La complessità e l'estrema dinamicità del tema renderebbero azzardato qualunque tentativo di trarre conclusioni; in tale sede, ci limiteremo, dunque, a seminare pochi semplici spunti, augurandoci che si rivelino utili in vista di future e più approfondite analisi.

premette l'importanza di «comprendere la natura del diritto all'oblio quale mera estensione del diritto alla *privacy* ovvero come diritto della persona», derivando, dall'una o dall'altra qualifica, differenze «sia dal punto di vista dell'estensione soggettiva, che della relativa tutelabilità»; sul punto, approfonditamente, anche Martinelli (2017), pp. 39ss.

[9] In generale, sulla 'funzione sociale' del diritto alla protezione dei dati personali e, corrispondentemente, sulla sua natura *relativa* dal punto di vista operativo, Ricci (2017), pp. 598ss.

[10] In tema, con particolare attenzione al bilanciamento tra conservazione dei dati e garanzia dei diritti fondamentali, Caggiano (2018), p. 64; Scaffardi (2017), p. 55; con specifico riferimento alla legittimità dell'acceso ai dati da parte dell'autorità giudiziaria, Formici (2018), p. 453.

[11] Corte giust. UE, sent. 8 aprile 2014, C-293/12 e C-594/12.

[12] Secondo Flor (2015), pp. 154s, 161, 168, dall'intersezione tra oblio e c.d. *data retention*, dovrebbe emergere una griglia di *standard* minimi che consentano di bilanciare il diritto alla *privacy* del singolo con le istanze di tutela della collettività.

[13] Art. 24 l. 20 novembre 2017, n. 167: «*In attuazione dell'art. 20 Dir. (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli artt. 51 co. 3*-quater*, e 407 co. 2 lett.* a *c.p.p. il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'art. 4*-bis *co. 1 e 2 d.l. 18 febbraio 2015, n. 7, conv. con mod. in l. 17 aprile 2015, n. 43, è stabilito in settantadue mesi, in deroga a quanto previsto dall'art. 132 co. 1 e 1*-bis *d.lgs. 30 giugno 2003, n. 196*».

[14] L'art. 11 co. 1 lett. *i* d.lgs. 101/2018 introduce l'art. 132 co. 5-*bis* d.lgs. 30 giugno 2003, n. 196, ai sensi del quale: «*È fatta salva la disciplina di cui all'art. 24 l. 20 novembre 2017, n. 167*». In proposito, è stato correttamente evidenziato che, non potendo il fornitore di servizi sapere in anticipo né quando né per quali reati gli verranno richiesti i dati, egli sarà comunque costretto a conservarli tutti per il periodo massimo di settantadue mesi. Ne discende, quanto ai tempi di conservazione, la sostanziale erosione dell'applicabilità dell'art. 132 co. 1 e 1-*bis* d.lgs. 196/2003 (Signorato (2018), p. 157).

[15] Il limite di sei anni previsto all'art. 24 l. 167/2017, ad avviso di Scaffardi (2017), pp. 83, 86, certifica una situazione di 'emergenza ordinaria'; allo stesso modo, Signorato (2018), pp. 157, 158. Di eccezione unica al mondo parla Barberio (2018), disponibile a questo link. Per alcuni profili di contrasto tra i principi espressi nella sentenza *Digital Rights Ireland* e il d.lgs. 196/2003 già prima della l. 167/2017, Flor (2017), pp. 360ss.

[16] Ciò non elimina, ovviamente, i punti di connessione tra sviluppo dell'identità (personale e digitale) e disciplina sulla *privacy*. In proposito, Resta (2007), pp. 521ss.

[17] Cass. civ. sez. I, sent. n. 978/1996.

2. La dialettica temporale tra processo penale e c.d. processo mediatico.

Con la locuzione 'processo mediatico', si è soliti indicare, in modo ampio e non senza enfasi[18], una modalità degenerata, da parte dei *mass media*[19], di fare informazione giudiziaria[20]: non già racconto critico del processo o dei fatti che ne stanno alla base[21], bensì vera e propria duplicazione di foro, forma perversa di giustizia parallela[22] che pretende di «scimmiottare liturgie e terminologie della giustizia ordinaria, riproducendone alcune cadenze, alcuni passaggi fondamentali»[23]. In questo senso, è stato efficacemente scritto, l'"aula mediatica' si costituisce come autentico foro alternativo[24].

Processo penale e processo mediatico condividono, al fondo, un tratto *narrativo*[25]: così come i *mass media* tendono alla costruzione della (di una) realtà sociale, contribuendo, al tempo stesso, alla stabilizzazione degli orientamenti cognitivi, normativi e valutativi della società stessa[26], anche nelle aule di giustizia si assiste alla *ri*-costruzione di un fatto sulla base di un ragionamento 'per storie'[27]. Sennonché, l'incedere impetuoso dei mezzi di comunicazione di massa, in tempi recenti, ha di fatto invertito i rapporti di forza tra questi due tipi di narrazione[28]; per certi versi, è anzi possibile affermare che oggi, in un'epoca caratterizzata prin-

[18] In tal senso, Riviezzo (2018), p. 64, che reputa il processo mediatico «un fenomeno di matrice eminentemente sociologica», pur senza negare le sue evidenti ripercussioni sul terreno propriamente giuridico. Circa gli effetti, rispettivamente, sul sistema giudiziario complessivamente preso e sul singolo processo, Giostra (2007), pp. 64ss; più di recente, Id. (2018b), p. 26ss.

[19] Fuoriesce dagli obiettivi del presente lavoro l'analisi delle 'anticipazioni di giudizio' da parte di soggetti pubblici *direttamente* coinvolti nelle indagini (forze dell'ordine, magistrati) mediante comunicati-stampa o conferenze. In tema, Mantovani G. (2013), p. 3787; Voena (2017), p. 1128.

[20] Il tratto degenerativo è confermato da numerosi esponenti di tutte le parti coinvolte nello *ius dicere* e nella sua narrazione. In dottrina, a conferma della grande lungimiranza del Siracusa Institute (all'epoca ISISC), rinviamo al dibattito, pionieristico, tra Cherif Bassiouni, Sergio, Fassone, Carponi Schittar, Ciruzzi e Pagliara (1996), pp. 193ss. Per quanto concerne l'avvocatura, sia sufficiente il rinvio al report, pubblicato nel 2016, *L'informazione giudiziaria in Italia. Libro bianco sui rapporti tra mezzi di comunicazione e processo penale*, a cura dell'Osservatorio sull'informazione giudiziaria dell'Unione Camere Penali Italiane (d'ora in avanti, UCPI). Nella magistratura, si segnala la presa di posizione netta, autorevole e dall'elevato profilo istituzionale di Canzio (2017), pp. 21s; da ultimo, Id. (2018), p. 1537. Quanto ai giornalisti, infine, si rinvia alle lucide parole di Ferrarella (2017), p. 4.

[21] Giostra (2007), p. 58; Id. (2018a), p. 8; per Turchetti (2017), p. 98s, «il processo mediatico non rappresenta […] un'espressione del diritto all'informazione (nelle sue componenti di diritto ad informare, ad essere informati, ad accedere alle informazioni), ponendo semmai un problema di rapporti con il diritto alla libera manifestazione del pensiero». Amodio (2016), p. 127, descrive la progressiva degenerazione dell'informazione giudiziaria come un *trend*: «Il peso sociale del giornalismo giudiziario è quindi a poco a poco cresciuto dando luogo ad una vera e propria invadenza denotata dalla ampiezza degli spazi operativi e da una complessa articolazione dei modi espressivi, approdati alla libertà di rielaborare autonomamente le notizie».

[22] «Accanto alla giustizia giudiziaria, lenta, tardiva, defatigante, indulgenziale, prospera una 'giustizia mediatica', rapida, sommaria, inquisitoria, senza contraddittorio, difesa, appello» (Mantovani F. (2015), pp. 288s). Secondo un Autore, la mediatizzazione estrema della giustizia comporta il «progressivo scivolamento da una dimensione di circolo virtuoso, nella quale i mezzi di comunicazione di massa contribuiscono a realizzare il precetto della pubblicità processuale (*trial with the media*), ad un circolo vizioso, ove la cointeressenza tra operatori della giustizia e organi di informazione fa sì che i processi vengano celebrati sui *media* ben prima che nelle aule giudiziarie» (Resta (2010), p. 18).

[23] Giostra (2007), p. 59.

[24] Giostra (2007), p. 59. Sulla sostanziale vicinanza tra racconto d'un ipotetico fatto di reato prescindendo dalle cadenze del processo e allestimento di una vera a propria 'meta-rappresentazione' giudiziaria, Conti (2016), pp. 7ss. La stessa giurisprudenza ha da tempo preso atto di questa 'dimensione parallela' della giustizia penale: «*secondo un fatto di costume oggi invalso e, comunemente, accettato, è consentito pure rivisitare in* talk show *televisivi gravi fatti delittuosi oggetto di indagini e persino di processo, nella ricerca di una verità mediatica in parallelo a quella sostanziale od a quella processuale. Iniziative di siffatto genere riscuotono, a quanto pare, apprezzabili indici di gradimento nell'utenza e sembrano inserirsi in un singolare fenomeno mediatico che tende a offrire una realtà immaginifica o virtuale, capace, nondimeno, per forza di persuasione, di sovrapporsi – ove acriticamente recepita dagli utenti – a quella sostanziale o, quanto meno, a collocarsi in un ambito in cui i confini tra immaginario e reale diventano sempre più labili e non facilmente distinguibili*» (Cass. pen. sez. V, sent. n. 45051/2009).

[25] Tale caratteristica parrebbe dipendere dalla circostanza che tanto il diritto penale quanto i *mass media* svolgono, ciascuno ai propri fini e coi propri strumenti, una funzione *comunicativa* e una funzione *performativa*, vale a dire di costruzione di realtà sociale. In tal senso, le illuminanti riflessioni di Hassemer (2004), pp. 159ss; in scia, autorevolmente, Paliero (2006), pp. 470, 481ss, 515ss; Palazzo (2009), pp. 194s; Bertolino (2012), p. 613. Del resto, la comunicazione è «di per sé un'ermeneutica, che si modifica a seconda dei contenuti, dei contesti, della rappresentazione» (Padovani (2008), p. 689).

[26] Luhmann (2001), part. pp. 41ss. Secondo il linguista Loporcaro (2005), pp. 15ss, la crisi della rappresentazione mediatico-criminale deriverebbe dalla prevalenza della 'notizia-racconto' rispetto alla 'notizia-informazione'.

[27] Forza, Menegon, Rumiati (2017), pp. 175ss, part. 201ss. Sebbene l'attenzione sia solitamente focalizzata sull'ermeneutica giudiziale, infatti, è bene ricordare che «anche le parti, non solo il giudice, sono fabbricanti di interpretazioni. La decisione giudiziale (teoricamente imparziale, obiettiva) nasce dal confronto e dal conflitto di posizioni diverse, 'di parte', che nel discorso pubblico accampano pretese di validità obiettiva, ma ha un fino *strategico*, orientato (con piena legittimità) ad un risultato pratico che corrisponda al meglio (nella situazione data) all'interesse di parte» (Pulitanò (2013), p. 134, corsivo nell'originale). Sull'intreccio *narrativo* tra diritto e letteratura, tanto in prospettiva ermeneutica quanto etico-valoriale, Visconti (2017), pp. 67ss, part. p. 73, sul ruolo dell'operatore del diritto.

[28] Resta (2010), p. 20. Inversione analoga, del resto, si verifica anche sul piano politico-criminale. Scrive Paliero (2012), pp. 116s: «L'idea che i *media* siano oggetto di una strumentalizzazione da parte degli esponenti politici è ampiamente superata: è il legislatore penale stesso che è *geneticamente* un *legislatore mediatico* o lo è diventato per ragioni di alleanza e/o di sopravvivenza nel teatro politico. […] È l'essenza

cipalmente da esperienze *mediate*[29], «le rappresentazioni (non solo mediatiche!) *del* crimine diventano *il* crimine con cui ciascuno di noi si confronta quotidianamente, a prescindere dalle reali esperienze individuali»[30]. In quest'ottica, la *mediatizzazione* della giustizia[31] sembra costituire una sorta di *upgrade* del predominio processuale sul diritto sostanziale[32]; prosecuzione naturale[33] di un unico composito movimento tellurico che approfondisce la faglia tra giustizia normativa, giustizia applicata e giustizia percepita[34].

Sebbene entrambi orientati alla ricostruzione di un determinato accadimento storico mediante specifiche tecniche narrative, tra processo penale e processo mediatico sussistono differenze di tipo strutturale e funzionale[35]. Decisiva, per quel che qui interessa, la loro diversa relazione col tempo: alla *diacronia* del processo, infatti, si è soliti contrapporre la tendenziale *sincronia* dei *mass media*. Mentre la giustizia penale è diluita nel tempo, argomenta un illustre studioso, «la definizione e il 'giudizio' dei *media* su di un 'fatto criminale' sono […] resi *definitivi* dalla notizia che 'vive', nella realtà mediatica, sin che è attuale»[36]; condizionata da pressanti logiche commerciali[37], la notizia si fa deperibile e, perciò, inadatta a sopravvivere oltre la soglia delle primissime fasi processuali[38]. Nel processo mediatico, insomma, il momento di reale afflittività si consuma istantaneamente, all'inizio - spesso, *soltanto* all'inizio - del procedimento vero e proprio.

La tensione temporale fra giustizia penale e giustizia mediatica si fa particolarmente elevata quando il mezzo di riferimento è internet. In linea generale, l'avvento della tecnologia ha impresso una svolta epocale ai processi di memorizzazione: originariamente circoscritta alla sfera individuale, la memoria è pian piano divenuta un autentico rituale collettivo[39], improntato a logiche di condivisione e interattività[40]. Tuttavia, considerato come sistema di memorizzazione, internet presenta caratteristiche che lo differenziano sia dalla memoria umana che da quella dei calcolatori[41]: la memoria di internet, nello specifico, è stata descritta come

mediatica di questo legislatore, in primo luogo, a dettare l'agenda politica selezionando così le *materie* (i *valori*) da assegnare *prioritariamente* alla competenza del sistema penale; e, in secondo luogo, a imbastire – nella superficialità 'opinionistica' dell'arena mass-mediatica, libera dai vincoli del confronto parlamentare – il *modo di disciplina* (soprattutto nel richiamato sbilanciamento sull'autore) e il *lessico* (bellico e non riconciliativo)» (corsivi nell'originale).

[29] Giostra (2007), p. 60, il quale considera un ossimoro ritenere *immediata* la forma di 'giustizia' «mediata per definizione e per eccellenza». Sul punto, significativo notare, quanto alle riprese audiovisive dei processi, che «l'effettivo significato della pubblicità immediata dei dibattimenti si risolve oggi nel predisporre le condizioni materiali perché possa esercitarsi con efficacia la pubblicità mediata» (Voena (2017), p. 1115).

[30] Paliero (2006), p. 504 (corsivi nell'originale); analogamente, Bertolino (2012) p. 612; Giostra (2018b), p. 32. Ciò, è evidente, pone problemi particolarmente delicati, giacché i *media*, per loro natura, agevolano ed esaltano le *defaillance* cognitive tipiche della conoscenza istintuale in possesso dell'utente medio (Conti (2016), p. 4); sui riflessi della comunicazione mediatica del crimine sulla 'gestione psicologica del male criminale', Palazzo (2018), pp. 17s. In prospettiva psicologica, anche i rilievi di Forza, Menegon, Rumiati (2017), pp. 192ss.

[31] Intesa, qui, come attribuzione al fatto rappresentato dai *media* «'*second code*' parallelo e talvolta 'alternativo' a quello espresso dal legislatore penale nella norma comportamentale e nella strumentale norma organizzatoria-processuale» (Paliero (1990), p. 508; successivamente, anche in Id. (2006), p. 493). Della 'mediatizzazione della giustizia' quale «malmesso recinto semantico» nel quale confluiscono una molteplicità di fenomeni sì eterogenei, ma comunque accomunati dell'individuazione in un certo strumento mediatico un foro alternativo, Giostra (2018a), p. 9.

[32] È noto che, alla tendenziale ineffettività dello studio teorico del diritto sostanziale, si accompagna ormai la «esaltazione del processo, quale *realtà* e, dunque, *verità*, del diritto» (Gargani (2017), p. 60). Sul tema, nella sconfinata letteratura, si rinvia al recente dibattito con interventi di Giunta, Micheletti, Bernasconi, Pulitanò, Tarli Barbieri, Velluzzi, Violante e Zilletti (2016), pp. 157ss. Per un'efficace sintesi sulla combinazione problematica tra incertezza del dato normativo e pro-attivismo giudiziario, da ultimo, Coppola (2018), pp. 1639ss.

[33] Puntualizzano le stringenti connessioni tra 'processualizzazione' del diritto e *mass media*, Caterini (2013), pp. 614ss; Gargani (2017), pp. 60, 71; Palazzo (2012), p. 1610.

[34] Sulla triade giustizia *normativa* (il dover essere), giustizia *amministrata* (l'essere) e giustizia *percepita* (la rappresentazione), Giostra (2016), p. 77.

[35] In dottrina, anche per un inquadramento della dicotomia diritto penale/*mass media* oltre la dimensione processuale, Paliero (2006), p. 490 ss; Giostra (2007), p. 59; Id. (2018a), pp. 26ss; Id. (2018b), pp. 4s; Palazzo (2009), pp. 195ss, 204ss; Padovani (2008), pp. 689s; Bertolino (2012), pp. 612ss; Bianchetti (2018), pp. 327ss.

[36] Paliero (2006), p. 491s (corsivi nell'originale); analogamente, Bertolino (2012), p. 614.

[37] Su politica criminale, logiche commerciali e *marketing*, Bertolino (2003), p. 1081; Caterini (2013), pp. 607ss; Bianchetti (2018), pp. 64ss.

[38] Giostra (2007), pp. 61s; Palazzo (2009), p. 206; Padovani (2008), p. 691 parla dell'immediatezza dell'informazione come di «una sorta di reazione 'ansiogena'» alla lunghezza biblica dei processi penali: «La presunzione di non colpevolezza, si rileva, assisterà il soggetto sino alla sentenza definitiva, ma il giudizio politico e sociale non si fonda sempre sull'attribuzione di una responsabilità penale: si riferisce anche a condotte errate e inopportune, eticamente riprovevoli».

[39] In tema, Resta e Zeno-Zencovich (2012), pp. 11, part. 38ss; Rodotà (2012a), pp. 211ss; Rodotà (2012b), p. 497. Sui limiti della memoria quale rituale condiviso, in senso critico, Pugiotto (2009), pp. 11ss.

[40] In psicologia cognitiva, si tende a parlare di 'memoria transattiva', con ciò intendendo un modello di attività mnemonica espansiva affidata a una pluralità di menti. Stando a recenti studi, «internet è diventata la nostra principale forma di memoria *esterna* o *transattiva*, come luogo esterno a noi stessi ove le informazioni sono immagazzinate» (Sparrow - Liu - Wegner (2011), p. 776). Con riferimento all'oblio, Korenhof et al. (2014), part. pp. 4ss.

[41] Bonavita (2016), pp. 34ss.

immensa, universale, disorganizzata, densa, volatile e, per quel che qui più interessa, *persistente*[42]; in internet, «a causa dell'immane permanenza delle tracce, il passato assume un nuovo significato, ma vi è anche una nuova e potente capacità di diffusione della notizia» che rende la cancellazione, sempreché normativamente consentita, «un'impresa che solo in alcuni casi di diffusione limitata del contenuto potrà essere portata a compimento in modo efficace»[43]. Oltre ad aumentare la capillarità di diffusione, insomma, internet conferisce alle notizie una spiccata «latenza passiva, che […] dilata la sfera della disponibilità virtuale»[44].

La potenzialità lesiva della circolazione via *web* d'informazioni relative a ipotetiche responsabilità penali deriva proprio dall'intreccio dei due tratti appena accennati[45]: la combinazione fra istantaneità (del processo mediatico) e persistenza (della memoria virtuale), in effetti, fa sì che, su internet, le *notitiæ* (non necessariamente) *criminis*[46] possano non soltanto permanere, ma permanere, come efficacemente precisato, «solo nelle premesse»[47], senza che agli eventuali successivi sviluppi (ad es., un decreto di archiviazione) sia dato adeguato peso.

In definitiva, il 'casellario' di internet presenta un'accentuata resistenza selettiva, in grado di cristallizzare le (sole) fasi iniziali di una determinata vicenda penale, con conseguente distorsione del quadro complessivo, inquinamento del corretto svolgimento del rito *reale* e, in ultimo, sacrificio dei diritti dei soggetti coinvolti.

3. L'evoluzione del diritto all'oblio.

Le modalità di memorizzazione di internet reclamano strumenti che mettano il titolare dei dati personali nella condizione di esercitare la propria libertà informatica; ed è proprio nel tratto che congiunge libertà informatica 'negativa' e libertà informatica 'positiva' che, ad avviso di accorta dottrina, germoglia il c.d. diritto all'oblio[48]. Concepita come virtù - nelle parole del Sommo - «che toglie altrui memoria del peccato», complice la rapida evoluzione tecnologica, l'oblio ha in realtà assunto forme e significati sempre nuovi e via via più complessi; tutti, ad ogni modo, in qualche misura agganciati alla tutela dell'identità personale. È opportuno, seppur in estrema sintesi, dar conto di quattro passaggi-chiave.

(I) Secondo una prima accezione, elaborata in tempi precedenti all'irruzione del *web*, il diritto all'oblio rappresenta una costola del diritto alla riservatezza[49] e mira a soddisfare, come suggerisce la versione in inglese, la pretesa del singolo di essere dimenticato - forse più correttamente: di non essere ricordato. In questo senso, l'oblio declina quell'istanza di *solitudine* che, come magistralmente scritto, garantisce «le condizioni che consentono a ciascun cittadino di non essere soltanto protetto nella sua sfera privata, ma davvero libero anche nella sfera pubblica»[50]. Così interpretato, il diritto all'oblio è stato invocato al fine di non vedere riproposte informazioni temporalmente risalenti qualora mancasse l'interesse attuale alla loro ripubblicazione[51].

[42] Martinelli (2017), pp. 15s.
[43] Martinelli (2017), p. 24. Si pensi, a titolo d'esempio, alle difficoltà di rimozione di informazioni ripubblicate, condivise da numerosi utenti oppure 'banalmente' duplicate mediante lo strumento della c.d. copia *cache*.
[44] Pardolesi (2017), 85; di «memoria sociale che si dilata all'infinito», parla anche Thiene (2017), p. 426; analogamente, Resta (2014), pp. 892s e bibliografia ivi richiamata.
[45] Sull'istantaneità e l'atemporalità delle comunicazioni in rete, già Castells (2002), pp. 525ss.
[46] I *mass media* sembrerebbero portare a estreme conseguenze la 'notizia di reato' quale costrutto «periclitante tra l'apparenza e la possibilità: due valutazioni la cui capacità denotativa è inconsistente, ma sulle quali si edifica un potere immane ed enorme di collegamento tra legalità e giurisdizione, il potere d'accusa. Un potere che rende il pubblico ministero arbitro e protagonista di una vicenda procedimentale in cui spesso si esprime e si condensa l'intero meccanismo della reazione repressiva» (Padovani (2001), p. 585).
[47] Marandola (2017), p. 373.
[48] Frosini (2012), pp. 912ss; in prospettiva più ampia, Id. (2017), p. 657.
[49] Più precisamente, Pietropaoli (2017), p. 70, evidenzia che il diritto all'oblio non è «una mera espressione del diritto alla riservatezza, ma di quest'ultimo è piuttosto una proiezione, una variante, un riflesso».
[50] Rodotà (2006), p. 100. Scrive il chiaro Autore che l'oblio è la vita che «chiede soccorso al diritto per evadere da se stessa, per non divenire prigioniera delle rete tecnologica dalla quale sempre più largamente ci troviamo avvinti» (*op. ult. cit.* p. 64).
[51] Afferma la Cassazione che, riconoscendo il diritto all'oblio, l'ordinamento protegge «*il giusto interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata*», salvo che non sopraggiungano fatti nuovi a far tornare d'attualità l'informazione (Cass. civ. sez. III, sent. n. 3679/1998). Più di recente, la Corte ha ribadito che «*il diritto dell'interessato* ad essere dimenticato *intanto può cedere il passo rispetto al diritto di cronaca in quanto sussista un interesse* effettivo ed attuale *alla diffusione della notizia; diversamente argomentando, altrimenti, si finirebbe col riconoscere una sorta di automatica permanenza dell'interesse alla divulgazione, anche in un contesto storico completamente mutato*» (Cass. civ. sez. III, sent. n. 16111/2013). Sulla principale casistica a partire dalla seconda metà degli anni Novanta, Ferola (2012), pp. 1010ss.

Non si tratta, ovviamente, di diritto assoluto[52]: il riconoscimento dell'oblio postula, dapprima, la stima di quanto tempo sia necessario affinché un fatto del passato possa essere relegato nell'ombra; quindi, un bilanciamento tra tutela della persona e libertà d'informazione, *sub specie*, alternativamente, di diritto cronaca (laddove il fatto passato sia inscindibilmente legato a un fatto attuale) ovvero di cronaca/critica storica (laddove il fatto passato sia storicamente rilevante).

(II) La rivoluzione digitale ha indotto una profonda mutazione dei contenuti dell'oblio: posto che, come accennato, su internet i problemi sorgono non tanto per via del tempo trascorso tra pubblicazione e ripubblicazione quanto, semmai, per via del tempo di *permanenza* dell'informazione, l'esigenza che sta alla base del diritto all'oblio «non è quella di non pubblicare, ma quella di *collocare* la pubblicazione, avvenuta magari legittimamente molti anni addietro, nell'attuale presente»[53]. Più che alla pretesa di essere dimenticati, dunque, il diritto all'oblio dà corpo all'istanza di esatta contestualizzazione della propria immagine, limitando e correggendo il processo di «continua cessione del sé agli altri» nell'ottica di protezione della propria dignità personale[54]. Come efficacemente scritto, insomma: «si chiede oblio e si ottiene memoria (seppur contestualizzata)»[55] nel segno d'una inedita «*concezione* dinamica *della riservatezza*»[56].

(III) Un punto di svolta nella recente evoluzione del diritto all'oblio in rete è indubitabilmente segnato dalla sentenza *Google Spain*[57]. Nella fondamentale pronuncia, resa sotto la vigenza della precedente Dir. 95/46/CE, la Corte di Giustizia delinea una sorta di 'mini-statuto' per motori di ricerca, stabilendo che: *(i)* l'attività del motore di ricerca dev'essere considerata 'trattamento' (§§ 26-31) e il motore stesso dev'esserne considerato 'responsabile' (§§ 32-40); *(ii)* è applicabile la legge nazionale del Paese in cui un motore di ricerca opera (§§ 55-60)[58]; *(iii)* il titolare dei dati ha diritto di rivolgersi direttamente al motore di ricerca per chiedere la rimozione dei risultati che rinviino verso pagine contenenti informazioni personali, anche laddove tali informazioni siano state lecitamente pubblicate e non vengano simultaneamente rimosse dalla pagina-origine (§§ 66-88).

Non è questa le sede per dar conto di pregi, difetti e ricadute della sentenza[59]. Ai nostri limitati fini, è sufficiente sottolineare che essa rimodula significativamente la pretesa d'oblio[60]: coniugando, di fatto, istanze di rimozione e di rettifica, la procedura di c.d. de-indicizzazione mira a proteggere l'individuo dalla penetrante ingerenza dei motori di ricerca, offrendogli la possibilità di intervenire, 'per sottrazione', nell'inesauribile processo di costruzione della sua identità digitale[61].

Anche così interpretato, ad ogni modo, il diritto all'oblio in rete dev'essere bilanciato col contrapposto diritto fondamentale a dare e ricevere informazioni[62]. A tal fine, sovvengono le *Linee guida* stilate dal c.d. *Working Party* 29 (WP 29)[63] per l'implementazione della stessa sentenza *Google Spain*[64]; nel documento, vengono elencati i criteri - elaborati a partire dalla

[52] Sui punti chiave del bilanciamento tra diritto all'oblio e diritto all'informazione nell'ordinamento italiano, per tutti, ancora Ferola (2012), pp. 1005ss.
[53] Finocchiaro (2015), p. 31.
[54] Per questo spunto, Rodotà (2012a), pp. 222s.
[55] Pietropaoli (2017), p. 73.
[56] Cass. civ. sez. III, sent. n. 5525/2012. Scrive Vesto (2018), p. 111: «questo accade anche perché all'identità (che si incastrava perfettamente nel precedente momento storico, ma non più nella condizione contemporanea) oggi sembra sostituirsi l''identificazione', concepita come (non un prodotto finito ma) un incessante e infinito processo di riproduzione e riciclo».
[57] Corte giust. UE, sent. 13 maggio 2014, C-131/12.
[58] Sui limiti territoriali dell'obbligo di rimozione, tuttavia, da ultimo, Corte giust. UE, sent. 24 settembre 2019, C-507/17. Di «passo indietro […] legat[o] in qualche modo alla necessità di rimediare agli errori precedenti», parla, in sede di prima lettura, Pollicino (2019).
[59] Per un ricco affresco, si rinvia ai lavori, in parte già citati, di Frosini, Pollicino, Finocchiaro, Caggiano, Piroddi, Sartor - De Azevedo Cunha, Mantelero, Sica - D'Antonio, Comella, Riccio, Flor e Pizzetti (2015); in aggiunta, Miniussi (2015), p. 209; Martinelli (2017), pp. 125ss; in tono critico, Pardolesi (2017), pp. 77ss.
[60] In un'intervista su Il Sole 24 Ore resa all'indomani della sentenza, il Presidente dell'Autorità Garante per la *privacy* Antonello Soro spiegava: «Uno dei meriti dell'intervento dei giudici europei [...] è che il diritto all´ oblio è stato riconosciuto come tale. Non è più una suggestiva espressione utilizzata nei dibattiti tra giuristi o nell'ambito giornalistico: è un diritto che ha immediate ricadute sulla dignità personale e sulla protezione dei dati».
[61] Si tratta di un diritto importante, considerata la naturale tendenza degli utenti a reputare le scelte d'indicizzazione affidabili, rilevanti e neutrali. Sul punto, Pitruzzella (2018), p. 25.
[62] *Amplius*, Martinelli (2017), pp. 185ss; in toni critici, Pollicino (2018), pp. 59ss.
[63] L'*Article 29 Data Protection Working Party* (più semplicemente *Working Party* 29), formato sulla base dell'art. 29 Dir. 95/46/CE, rappresenta il gruppo di lavoro comune delle autorità nazionali europee in materia di vigilanza e protezione dati. Il Reg. 679/2016/UE (GDPR) lo ha ribattezzato *European Data Protection Board* (EDPB), individuando all'art. 70 i suoi compiti.
[64] Article 29 Data Protection Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on*

casistica precedente - che le autorità nazionali possono adoperare, in linea con la legislazione domestica, come «strumenti di lavoro flessibili» per contemperare i princìpi enucleati dalla Corte e l'interesse del pubblico ad avere accesso all'informazione[65]. Stando alla griglia delineata dal WP 29, in particolare, all'autorità nazionale è richiesto di valutare l'eventuale ruolo pubblico rivestito dal soggetto (n. 2), l'accuratezza e l'aggiornamento del dato (nn. 4 e 7), la natura eventualmente eccessiva del trattamento (n. 5), il contesto all'interno del quale l'informazione è stata pubblicata (nn. 10-11) e la portata del pregiudizio arrecato al soggetto citato (n. 8). Tali criteri vanno modulati e combinati alla luce del caso concreto; il mero decorso del tempo, precisa tuttavia il WP 29, non è di per sé risolutivo, rilevando, piuttosto, se la permanenza del dato sia in linea con la finalità originaria del trattamento[66].

(IV) L'ultimo tassello di questo tortuoso percorso è dato dalla positivizzazione del diritto all'oblio all'interno del Reg. (UE) 679/2016 (GDPR); una positivizzazione, per la verità, soltanto apparente, posto che la rubrica dell'art. 17 GDPR recita 'Diritto alla cancellazione' e confina la dicitura 'diritto all'oblio' tra parentesi[67]. La disciplina per la rimozione dei dati si presenta piuttosto articolata. Ai nostri fini, si segnala che: *(i)* l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati che lo riguardano senza ingiustificato ritardo laddove, in particolare, essi non siano più necessari per la finalità per cui vennero trattati (art. 17 § 1 lett. *a*); *(ii)* il titolare del trattamento obbligato alla cancellazione è altresì obbligato ad adottare «*le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi* link*, copia o riproduzione dei suoi dati personali*» (art. 17 § 2); *(iii)* i dati non debbono essere cancellati laddove il loro trattamento risulti necessario per alcune finalità espressamente tipizzate (art. 17 § 3).

Non è possibile approfondire i risvolti problematici di un regime[68] che, a seconda delle opinioni, denomina in modo poco appropriato un diritto in realtà già esistente[69], condiziona l'operatività del diritto stesso a elementi incerti (es., «*la tecnologia disponibile*», «*i costi di attuazione*»)[70], ridimensiona le potenzialità assunte dall'oblio nell'elaborazione successiva alla sentenza *Google Spain*[71], rischia di favorire fenomeni di c.d. censura collaterale[72] e via dicendo. Senza con ciò voler disconoscere i punti deboli della disciplina, per quel che qui interessa, ci limitiamo a sottolineare che il GDPR, facendosi carico della potenziale diffusione e permanenza dei dati su internet: *(i)* regolamenta espressamente il diritto alla cancellazione; *(ii)* nell'elencare gli interessi contrapposti, riprende il binomio tradizionale valorizzando sia l'esercizio del diritto alla libertà di espressione e informazione (art. 17 § 3 lett. *a*), sia l'archiviazione nel pubblico interesse, di ricerca scientifica o storica ovvero a fini statistici (art. 17 § 3 lett. *d*)[73]; *(iii)* affianca al diritto di cancellazione/oblio altri diritti 'complementari'[74], attualizzati rispetto alla versione della Dir. 95/46/CE[75], complessivamente volti alla tutela della c.d. identità dinamica della persona[76]; *(iv)* in chiave generale, subordina ogni trattamento di dati personali al rispetto dei criteri di adeguatezza, pertinenza, esattezza, aggiornamento e conservazione per il solo tempo

'Google Spain and Inc. v. *AEPD and Mario Costeja González' C-131/12*, disponibile a questo link.

[65] Martinelli (2017), p. 195, sottolinea che la vera problematica affrontata nelle *Linee guida* attiene non alla responsabilità del motore di ricerca, né alle questioni definitorie della Dir. 95/46/CE, né infine all'individuazione del soggetto che sia in grado di 'cancellare' i contenuti lesivi, bensì alla «esigenza di porre un freno o, comunque, dei limiti all'invasione della *privacy* che i motori di ricerca veicolano, diminuendo i tempi della ricerca e consentendo un accesso rapido e 'facilitato' a un gran numero di informazioni relative ad una specifica persona».

[66] Approfonditamente, Korenhof e Al. (2014), pp. 9ss.

[67] Il collegamento stretto tra cancellazione e oblio è anticipato dai cons. 65 e 66.

[68] Un efficace quadro di sintesi è offerto da Agnino (2018), pp. 108s.

[69] Stradella (2017), p. 90, parla di denominazione «provocatoria e demagogica»; in senso analogo, sull'inesattezza del riferimento all'oblio, Rugani (2018), p. 464; Zanini (2018), pp. 12s, 19; Cuffaro (2019), p. 4.

[70] In chiave critica, di 'indefinito obbligo tecnologico' parlano Bonavita e Pardolesi (2018b), p. 277.

[71] L'art. 17 GDPR, in effetti, sembrerebbe: *(i)* restringere la portata del diritto all'oblio precedentemente inteso (anche) come diritto alla deindicizzazione o, più in generale, come diritto all'identità dinamica (Di Ciommo (2017), pp. 625ss; Thiene (2017), pp. 411s); *(ii)* sovvertire la gerarchia tra diritto all'oblio e libertà d'informazione, con quest'ultima destinata a prevalere in via pressoché automatica (Rugani (2018), pp. 460s; Stradella (2017), p. 89) relegare il motore di ricerca nella posizione di soggetto terzo cui *ex* art. 17 § 2 dev'essere 'semplicemente' comunicato l'avvio della procedura di cancellazione (in senso favorevole, Zanini (2018), pp. 14ss, 20).

[72] Bonavita e Pardolesi (2018b), pp. 279ss.

[73] Il delicato bilanciamento tra tutela dell'identità personale e tutela della *lato sensu* memoria storica è affidato all'art. 89 (*Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*), 'anticipato' dal cons. n. 156. Premessa l'importanza riconosciuta dal GDPR a tali finalità, è interessante sottolineare, da una parte, che il diritto alla cancellazione/oblio non figura tra i diritti che, a tali fini, possono subire deroghe; dall'altra, che il § 1 esplicita l'esigenza di rispettare il principio c.d. di minimizzazione dei dati (es., archiviazione mediante pseudonimizzazione).

[74] Art. 16 (*Diritto di rettifica*), art. 18 (*Diritto di limitazione di trattamento*), art. 21 (*Diritto di opposizione*).

[75] Si vedano, in particolare, gli artt. 12 e 14 Dir. 95/46/CE nonché, a livello domestico, il vecchio art. 7 co. 3-4 d.lgs. 196/2003.

[76] Di Ciommo (2017), pp. 627ss.

necessario (art. 5 § 1 lett. *c*, *d*, *e*).

In conclusione, al netto delle ambiguità semantiche e delle criticità operative, quest'evoluzione consente d'individuare un nesso di sostanziale strumentalità tra diritto all'oblio e tutela dell'identità personale: come è stato puntualizzato, difatti, il diritto all'oblio nasce sul terreno del conflitto tra storia e attualità col ruolo di presidio dinamico dell'identità personale, bene di sintesi, protetto nei suoi molteplici aspetti e nelle sue molteplici forme[77].

4. La figura della 'vittima mediatica': beni aggrediti e modalità d'aggressione.

Nel processo mediatico, lo abbiamo visto, il mezzo di comunicazione di massa pretende di farsi foro alternativo, delocalizzando lo spazio giudiziario e paralizzando il tempo[78]. Dentro questa cornice, prende forma un'inedita tipologia di vittima: la vittima, per l'appunto, *mediatica*[79]. Più che di c.d. vittimizzazione secondaria[80], si tratta, ci sembra, d'una artificiosa eterogenesi di ruoli[81], che porta colui che nell'ipotesi accusatoria riveste la parte di autore a divenire il principale danneggiato[82], sguarnito, peraltro, delle garanzie tradizionalmente assicurate alle parti processuali 'reali'[83]. Due, in estrema sintesi, gli aspetti pregiudizievoli.

In primo luogo, il risalto della vicenda criminale comporta una sovraesposizione del soggetto coinvolto; sovraesposizione, spesso, particolarmente segnante. Traslato sul piano fluido dei *mass media*, infatti, il fenomeno del 'processo come pena' subisce un'incontenibile amplificazione[84], specialmente quando il mezzo di riferimento è internet. In questo senso, la liturgia punitiva massmediatica, portata ai suoi estremi, sembra configurare un'inquietante riedizione tecnologica dello 'splendore dei supplizi', volta, ben più che a stigmatizzare il crimine, a far sì che «la memoria degli uomini […] serb[i] il ricordo […] della sofferenza dovutamente constatat[a]»[85]. La pubblicizzazione dei provvedimenti che stabiliscono responsabilità penali non è certo pratica nuova nel nostro ordinamento; va anzi ricordato che, proprio al fine di favorirne la visibilità, il novellato art. 36 c.p. prevede che le sentenze di condanna vengano pubblicate, per un periodo fino a trenta giorni, sul sito internet del Ministero della Giustizia. È, tuttavia, proprio dal confronto con la sanzione accessoria[86] che emerge, all'opposto, il carattere precipuamente stigmatizzante della 'pena mediatica'[87]: la misura di cui all'art. 36 c.p. segue una sentenza di condanna[88], confina la pubblicazione in un 'luogo' istituzionale ed è applicata

[77] Finocchiaro (2015), pp. 40s; Thiene (2017), p. 413.
[78] Così, sulla scia di Antoine Garapon, Fondaroli (2014), p. 143; approfonditamente, Amodio (2016), pp. 130ss.
[79] In tema, si veda il raffinato lavoro di Manes (2017), p. 114, che arriva a concepire la sottoposizione parallela a giudizio ordinario e giudizio mediatico come una sorta di *bis in idem* (p. 120); dall'angolo visuale privatistico, Tucci (2010), pp. 126ss.
[80] Con 'vittimizzazione secondaria', nelle scienze criminologiche, si suole riferirsi a una condizione di sofferenza psicologica vissuta dalla vittima di un reato durante l'*iter* giudiziario, non derivante direttamente dall'offesa subita bensì dalla risposta formale, conseguente al reato, adottata dalle istituzioni.
[81] Scrive Fondaroli (2014), p. 145, che, nell'anticipare il giudizio degli organi deputati, i protagonisti della vicenda processuale «sono costruiti artificialmente ed in modo arbitrario, condizionato dalle finalità e dagli orientamenti di chi imbastisce la trama della 'verità' da dare in pasto ad un pubblico sempre più famelico di (pseudo)democrazia diretta».
[82] Aprati (2017), p. 980, nell'analizzare le ricadute derivanti dalla sottoposizione a processo, distingue tra pregiudizi certi e pregiudizi eventuali, facendo rientrare nella seconda categoria anche i danni conseguenti alla rilevanza mediatica del caso.
[83] Con specifico riferimento ai 'processi su internet', da ultimo, Canepa e Ponton (2019), pp. 2ss. Sul processo mediatico in genere, Giostra (2007), p. 65, amaramente rileva che «quando lo scontro processuale si sposta sui mezzi di informazione, i più corretti tra i suoi protagonisti del processo [sono] i più svantaggiati e che quindi le sorti del processo, almeno a livello massmediatico, [dipendono] da fattori affatto diversi dalla consistenza delle prove a carico o a discarico». Sulla contrapposizione tra 'giusto processo' e 'ingiusto processo mediatico', con spunti diversi, Riviezzo (2018), part. pp. 69ss; Amodio (2016), pp. 135, 145ss; Conti (2016), pp. 10s. È appena il caso di ricordare, peraltro, che anche la vittima da reato, in conseguenza della Dir. 2012/29/UE, recepita in Italia con d.lgs. 15 dicembre 2015, n. 212, gode ora di garanzie procedurali più piene e meglio delineate.
[84] Bertolino (2003), p. 1077; Palazzo (2009), pp. 205s; sul potere punitivo *del* procedimento, di recente, Gargani (2017), pp. 68ss e bibliografia ivi richiamata.
[85] Foucault (1993), pp. 37s.
[86] Sebbene in tempi risalenti, la giurisprudenza ha riconosciuto che la pena accessoria della pubblicazione della sentenza «*risponde a razionali intendimenti quali la riparazione del danno non patrimoniale cagionato alla vittima, la salvaguardia di altre possibili vittime, la creazione nell'animo del reo di motivi di pentimento e di emenda scaturenti dalla divulgazione del suo trascorso*» (Cass. pen. sez. VI, sent. n. 7058/1974).
[87] Il parallelo emerge nelle calzanti parole di Zeno-Zencovich (2007), p. 271, il quale ravvisa nel processo mediatico la capacità di imporre «sanzioni reputazionali accessorie».
[88] «*Le pene accessorie conseguono di diritto alla sentenza di condanna come effetti penali della stessa ai sensi dell'art. 20 c.p., con la conseguenza che non possono essere mantenute in caso di proscioglimento dell'imputato, anche se pronunciato a seguito di estinzione del reato per prescrizione*» (Cass. pen.

in linea col principio di legalità[89]; la 'pena mediatica', viceversa, è emessa a giudizio in corso, è abbandonata ai flutti indomabili della rete ed è irrogata in spregio di qualsivoglia garanzia. In questa luce, l'esposizione da processo mediatico tende ad avvicinarsi, semmai, alle discusse *shaming sanctions*[90], consistendo, di fatto, nel principale risvolto d'un rituale para-giurisdizionale dai forti connotati simbolici teso a umiliare pubblicamente la vittima[91] e a incentivare la fiducia collettiva nella stabilità dell'ordine giuridico[92].

In secondo luogo, lo si è in parte già detto, i *mass media* arretrano il baricentro procedimentale alla fase delle indagini[93]. Verrebbe da dire: *preliminari* di nome, *centrali* di fatto. Accade così che le attività (unilateralmente)[94] svolte in fase d'indagine acquistino, agli occhi dell'opinione pubblica, un valore che esse, in un sistema accusatorio polarizzato sulla formazione della prova in dibattimento, non dovrebbero in realtà avere. Nel clamore mediatico intorno a un determinato caso giudiziario, dunque, ciò che da codice costituisce uno *step* intermedio (ad es., una misura cautelare) o addirittura un semplice atto d'impulso (ad es., l'invio dell'informazione di garanzia), al netto di inevitabili precisazioni di circostanza[95], finisce spesso per essere offerto alla collettività come acquisizione inconfutabile e irreversibile.

Quest'anticipazione, favorita dall'infelice disciplina sul segreto istruttorio[96], ha importanti ricadute in almeno due direzioni: per un verso, induce forze dell'ordine e magistrati a calibrare le indagini sui tempi frenetici dei *mass media*[97], costringendoli, in casi estremi, a cercare nel rito virtuale - rapido e sommario - una forma di giustizia *surrogatoria* rispetto a quella istituzionale - fisiologicamente più lenta e articolata[98]; per l'altro, veicola un'immagine dei soggetti coinvolti destinata a rimanere impressa nella mente dell'opinione pubblica, a prescindere da eventuali sviluppi processuali liberatori[99].

Le ragioni che cementano tale *pre*-giudizio possono attenere alla qualità dell'autore (alter-

sez. II, sent. n. 38345/2016).

[89] Sull'inapplicabilità della pena accessoria in caso di condanne per reati che non prevedano esplicitamente tale misura, Cass. pen. sez. I, n. 47216/2016; sull'inapplicabilità del nuovo art. 36 co. 2 c.p. ai fatti pregressi, Cass. pen. sez. II, sent. n. 14768/2017; Cass. pen. sez. II, sent. n. 4102/2016.

[90] Visconti (2011), pp. 636s, traccia nitidamente la linea di demarcazione tra pene accessorie in genere e cc.dd. *shaming sanctions*: al di là del loro diverso inquadramento giuridico, quest'ultime sono «caratterizzate da un *quid pluris* di stigmatizzazione, perché è proprio in funzione dell'esposizione del reo alla pubblica vergogna che esse vengono ideate e plasmate nei concreti contenuti […] la stigmatizzazione ne costituisce, cioè, l'obiettivo diretto e il carattere fondativo».

[91] Bertolino (2012), p. 632. Correttamente, Riviezzo (2018), p. 70, ritiene che «l'assenza di 'segretezza' […] non smentisc[a], ma anzi rafforz[i] la 'logica (larvatamente) inquisitoria' del nuovo rito mediatico che tanto preoccupa gli addetti ai lavori». Al contrario delle pratiche descritte da Foucault (1993), p. 50, peraltro, la 'pena mediatica' incentra il proprio potenziale lesivo non tanto sulla lentezza del supplizio quanto, come più volte ricordato, sull'istantaneità di un verdetto difficilmente 'appellabile'.

[92] Sulla vittimizzazione di massa e sulla funzione sedativo-unificante della pena in tempi di c.d. populismo penale, Pratt e Miao (2017), pp. 16s, 22s.

[93] Bertolino (2003), p. 1086; Giostra (2007), pp. 61ss; Id. (2018a), pp. 4s; Palazzo (2009), p. 206.

[94] Innegabile che «l'informazione collass[i] sull'accusa, che ne è in realtà l'unica fonte e ne rappresenta il baricentro ermeneutico» (Padovani (2008), p. 691). Approfonditamente, Amodio (2016), pp. 125ss, il quale ravvisa in buona parte della giustizia mediatica una vera e propria *apologia* del lavoro del magistrato inquirente come strumento di difesa della società dal delitto (pp. 128, 149).

[95] Clausole di stile, sì doverose ma vaghe e chissà quanto realmente convinte, tese a correggere, seppur in minima parte, il taglio inquisitorio impresso dalla stampa alla narrazione dei fatti di cronaca.

[96] Che la disciplina incerta e l'ineffettività delle sanzioni in caso di violazione rende «un'area di liceità di fatto» (Manes (2017), p. 116). In tema, nell'ampia letteratura, Amodio (2016), pp. 143s; Bartoli (2017), p. 59; Voena (2017), p. 1117s; Accinni (2018), pp. 175ss.

[97] Marafioti (2010), p. 113. Singolare la recente statuizione di un giudice di merito che ravvisa ne 'Le Iene' - programma di c.d. *infotaiment* storicamente votato alla spettacolarizzazione di potenziali vicende penali - uno «*strumento di ausilio investigativo* extra-ordinem *al fine di sottoporre all'attenzione dell'autorità giudiziaria l'eventuale commissione di reati*», salvo poi condannare i responsabili per un servizio che esorbitava «*dalla finalità puramente divulgativa della notizia, risolvendosi in una gratuita denigrazione della reputazione* […] *mirando sia ad inoculare e precostituire nel pubblico televisivo un pre-giudizio sulla colpevolezza del* [omissis] […] *sia ad alimentare nello spettatore una sensazione di disprezzo, non già verso condotte astrattamente qualificabili come delitti certamente esecrabili, bensì, direttamente nei confronti della persona umana additata come autrice di quelle stesse azioni, persona la cui dignità è presidiata da un nucleo essenziale meritevole di protezione incondizionata, anche a fronte dell'apparente commissione di gravi reati*» (T. Lucca, sent. n. 96/2019).

[98] Su questo rischio, concordemente, Paliero (2006), p. 533; Palazzo (2009), p. 207; Amodio (2016), p. 140; Giostra (2018a), p. 5, il quale parla, con toni particolarmente critici, di «reticolo carsico di reciproche compiacenze» tra soggetti pubblici coinvolti nel processo e testate giornalistiche. In senso complementare, peraltro, si osserva che l'anticipazione di giudizio alla fase preliminare parrebbe nascondere «una sorta di subliminale volontà 'risarcitoria'»: consapevole di non avere modo di seguire passo passo la vicenda, «il giornalista tende, per così dire, a 'compensare' il lettore pubblicando tutto e subito» (Giostra (2007), p. 63). In giurisprudenza, in termini netti, Cass. pen. sez. V, sent. n. 1105/2015, relativa al noto processo per l'omicidio di Meredith Kercher.

[99] Conti (2016), pp. 7s. Originariamente pensata come «complemento o completamento della sanzione» (Zeno-Zencovich (2007), p. 267), dunque, la comunicazione assume un ruolo sostitutivo, a tratti persino primigenio, cosicché non sembra esagerato parlare d'una vera e propria *anticipazione mediatica* della pena.

nativamente inviso[100] o in vista[101]), alla vulnerabilità della vittima[102], all'enormità del danno[103] o, sempre più spesso, alla particolare 'appariscenza' di un determinato elemento di prova[104].

Quale che sia l'origine, è dimostrato, comunque, che la progressiva divaricazione tra giustizia ordinaria e giustizia mediatica provochi «preoccupanti effetti dispercettivi»[105], in grado di incidere negativamente sulle prerogative del soggetto attinto da indagine penale[106]. Fra tali prerogative, figurano, in particolare, sia i diritti globalmente connessi alla personalità individuale (art. 2 Cost.)[107], sia, trattandosi di possibili coinvolgimenti criminali, la finalità rieducativa della pena (art. 27 co. 3 Cost.)[108] e, soprattutto, la presunzione di non colpevolezza (art. 27 co. 2 Cost.)[109]: nella sua accezione di 'regola di trattamento', difatti, quest'ultima assume «una valenza anche 'extra-processuale', quale fondamentale criterio di orientamento culturale»[110], che conferisce all'interessato il diritto a non essere illegittimamente *mostrato* come colpevole[111]. Tale declinazione, peraltro, trova oggi conferma, a livello sovranazionale, in una

[100] Si pensi, per restare alla stringente attualità, al caso di Desirée Mariottini, trovata morta in uno stabile abbandonato nel centro di Roma. Sui quattro indagati - stranieri, irregolari, occupanti abusivi di un'area pubblica e inseriti nel traffico di stupefacenti - la maggior parte dei *media* ha da subito calato il proprio irrefutabile verdetto di colpevolezza. Emblematica, in tal senso, la diffusione della notizia della cattura del quarto indagato, avvenuta una settimana dopo il ritrovamento del cadavere, a oltre trecento chilometri dal *locus commissi delicti* eppure, nell'immediatezza dell'arresto, non contornata da alcuna espressione dubitativa che lasciasse trasparire una mera *presunzione* di colpevolezza (che, peraltro, avrebbe di per sé costituito un'inversione del dettato costituzionale). Una risolutezza, crediamo, in larga parte dipendente dalla tipologia *deviante* degli autori, che consegna all'opinione pubblica quattro *sicuri* colpevoli, con buona pace dell'accuratezza che un caso tanto tragico e complesso richiederebbe.

[101] In un recente lavoro, Tripodi (2019), p. 272, ha incisivamente sottolineato che il c.d. populismo penale avrebbe, tra i suoi effetti, quello di determinare una vera e propria 'ipocondria giudiziaria' nell'agente pubblico o professionista di fascia medio-alta; a tale situazione della prassi corrisponde, come secondo emisfero d'un unico circolo vizioso, una maggiore visibilità giuridico-mediatica. Basti qui riportare il caso del dottor Brega Massone, al centro dello scandalo della casa di cura 'Santa Rita': originariamente dipinto come 'mostro', '*serial killer*', capo di una 'clinica degli orrori', il medico, nell'ultima *tranche* processuale (Ass. app. Milano sez. II, sent. n. 37/2018), ha visto significativamente ridimensionata la propria responsabilità; ai nostri fini, significativo, in particolare, il riconoscimento della «*semplicistica enfatizzazione massmediatica*» di cui l'imputato sarebbe stato oggetto. In controtendenza, per un'accurata ricostruzione già durante la fase delle indagini, Cracco e Pozzi (2011-2012), pp. 14ss.

[102] Sull'attenzione della vittima nella narrazione mediatica della giustizia, Paliero (2006), p. 502ss; Bertolino (2012), p. 617. In generale, sulla centralità della vittima nello scenario penalistico attuale, da ultimo, si veda il dibattito tra Pitch e Pugiotto (2019).

[103] Superata una fase di interesse relativamente più scarso (Bertolino (2003), pp. 1105s), evidente è, oggi, il *battage* mediatico nei procedimenti per reati ambientali (ad es., caso Ilva), o contro l'incolumità pubblica (ad es., la c.d. strage di Viareggio) o per fatti comunque connessi a calamità naturali (ad es., i procedimenti per omicidio colposo instaurati a seguito di un terremoto). Sulla contaminazione mediatica del diritto penale ambientale all'indomani dell'entrata in vigore della l. 68/2015, Catenacci (2015), p. 1077.

[104] Come autorevolmente scritto, la 'verità mediatica' trae la propria autorevolezza anche dal «superamento della forza della prova dichiarativa (da sempre precaria, ma da ultimo spesso pure smentita) a vantaggio della prova scientifica (meglio, tecnica)» (Spangher (2016), p. 807). Con riferimento ai *talk show*, ad esempio, si è sottolineato l'insistenza di dibattiti «che durano ore e sono incentrati millimetricamente su indizio che viene scomposto e vivisezionato in modo completamente avulso dal complesso indiziario, perdendo ogni reale significato di prova» (Marafioti (2010), p. 116). Stessa cosa può essere detta per la circolazione di 'materiale probatorio' su siti internet assai spesso non specializzati né in senso tecnico-scientifico, né in senso tecnico-giuridico. Basti l'esempio - attualissimo e drammatico per la portata dell'evento che ne fa da base - dell'insistenza dei *media* sulle prime relazioni tecniche circolate all'indomani del crollo del Ponte Morandi di Genova.

[105] Giostra (2018b), p. 27.

[106] Già in tempi relativamente meno recenti, scriveva Hassemer (2004), p. 148: «Alla sfera privata sono più o meno interessati tutti i *media*. Certo, non alla sua conservazione e difesa, ma al suo svelamento, vale a dire, alla sua parziale rimozione, alla sua limitata e temporanea distruzione».

[107] Tucci (2010), pp. 129ss.

[108] In questo senso, *a contrario*, le Sezioni unite civili hanno da ultimo cassato una sentenza che, in merito alla rievocazione di una vecchia vicenda di cronaca nera, aveva ritenuto prevalente il diritto di cronaca storiografica senza minimamente considerare «*nel bilanciamento delle contrapposte tutele, la bontà del percorso di riabilitazione che [l'attore] aveva compiuto nei ventisette anni intercorsi tra la prima e la seconda pubblicazione, scontando una lunga pena detentiva e reinserendosi, con tutte le comprensibili difficoltà che questo comporta, nel tessuto sociale produttivo*» (Cass. civ. sez. un., sent. n. 19681/2019).

[109] Nella contraddizione tra tempi dei *media*, tempi delle indagini e tempi della decisione, è stato autorevolmente sottolineato, «s'annida il conflitto tra la giustizia 'attesa' e la giustizia 'applicata', con il pernicioso ribaltamento della presunzione d'innocenza dell'imputato» (Canzio (2017), p. 21); ancor più criticamente, Amodio (2016), p. 134s, il quale correttamente evidenzia che «se […] l'informazione sulla giustizia penale è puntata esclusivamente sulla fase anteriore al giudizio, è la materia prima lavorata a trascinare il giornalista nel gorgo della presunzione di colpevolezza». Sulla lesione della presunzione d'innocenza, in senso conforme, Giostra (2007), p. 64; Resta (2010), pp. 42ss; Bertolino (2012), p. 626; Manes (2017), p. 117; Voena (2017), p. 1127s; ritiene che la presunzione d'innocenza, così intesa, tenda ad avvicinarsi molto alla reputazione Palazzo (2017), p. 145.

[110] Paulesu, (1995), p. 678.

[111] Come perfettamente spiegato dal Supremo Collegio, «*ogni individuo coinvolto in indagini di natura penale è titolare di un interesse primario a che, caduta ogni ragione di 'sospetto', la propria immagine non resti offesa da notizie di stampa che riferiscano dell'iniziale coinvolgimento e ignorino, invece, l'esito positivo delle stesse*» (Cass. pen. sez. I, sent. n. 14062/2008). È importante sottolineare, peraltro, che la lesione del diritto alla presunzione d'innocenza non viene meno laddove, nel prosieguo, si accerti effettivamente la responsabilità penale dell'imputato; precisa infatti la Cassazione che la verità del fatto, quale espressione del lecito esercizio del diritto di cronaca, si misura avendo riguardo al momento in cui la notizia viene divulgata, senza che abbiano rilievo eventi successivi (Cass. civ. sez. III, sent. n. 12013/2017). In dottrina, sulla valenza extra-processuale della presunzione d'innocenza, Mantovani, G. (2016), pp. 128s; per un primo riconoscimento da parte della Consulta, Corte cost., sent. n. 18/1966.

Raccomandazione del Consiglio d'Europa sull'informazione relativa a procedimenti penali[112] e, soprattutto, nella Dir. (UE) 343/2016[113], la quale - sebbene in relazione alle dichiarazioni delle pubbliche autorità - sembra ridisegnare il rapporto tra presunzione d'innocenza e divulgazione d'informazioni giudiziarie in termini di regola/eccezione[114].

Nel complesso, viene dunque a delinearsi un ampio 'diritto all'immagine sociale e giuridico-mediatica'[115], operante sia in chiave *ex-ante* sia, per quel che qui più interessa, in chiave *ex-post*[116]. In linea con l'evoluzione tratteggiata *sub* § 3, tale macro-diritto mira a schermare il titolare da rappresentazioni decontestualizzate accessibili a chiunque, mantenendo il rapporto tra la persona e il suo 'corpo digitale' e inspessendo, così, quel fitto groviglio di valori facenti globalmente capo al concetto di 'dignità'[117].

5. La tutela della vittima mediatica. Perimetrazione dell'indagine.

La permanenza a oltranza di notizie 'colpevoliste' detta una nuova combinazione al trinomio diritto/memoria/pena[118]: da possibile (e discusso) oggetto di tutela penale[119], nell'era dei 'processi su internet', la memoria diviene essa stessa strumento d'aggressione di diritti fondamentali. Riprendendo un'efficace immagine, insomma, la comunicazione di massa radicalizza il passaggio dalla *damnatio memoriæ* alla *memoria damnata*[120].

Ma quali forme assume quest'aggressione? A quali condizioni la vittima mediatica può invocare la lesione delle proprie prerogative? E quali le sedi ove reclamare il proprio diritto a 'rimanere nell'ombra'? Prima di rispondere a tali quesiti, s'impongono un paio di notazioni preliminari.

Anzitutto, preme anticipare che, ai fini del presente lavoro, assumono rilievo le informazioni *vere* originariamente pubblicate in modo *legittimo*: anche ammettendo l'estrema ampiezza del concetto, in effetti, le *rationes* alla base del diritto all'oblio non paiono sovrapponibili né a quelle relative alla tutela da cc.dd. *fake news*[121], né a quelle relative alla tutela del segreto processuale[122]. Vale la pena precisare, tuttavia, che tali traiettorie, all'atto pratico, tendono sovente

[112] Recommendation REC (2003) 13 of the Committee of Ministers to Member States, *On the Provision of Information through the Media in Relation to Criminal Proceedings*, 10 luglio 2003, part. art. 2 (*Presumption of Innocence*), art. 8 (*Protection of Privacy in the Context of Ongoing Criminal Proceedings*), art. 9 (*Right of Correction or Right of Reply*) e art. 7 (*Regular Information during Criminal Proceedings*), ove si sancisce che, nei procedimenti penali di lunga durata, l'informazione dev'essere resa regolarmente, per evitare che l'attenzione sia concentrata nella sola fase iniziale.

[113] Direttiva (UE) 343/2016 del Parlamento e del Consiglio, del 9 marzo 2016, *Sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali*, part. cons. nn 17-19 e art. 4 (*Riferimenti in pubblico alla colpevolezza*).

[114] Valentini (2016), p. 198.

[115] Marandola (2017), p. 375.

[116] In chiave *ex-ante*, tutelando l'individuo dalla prematura diffusione di notizie colpevoliste; in chiave *ex-post*, imponendo l'aggiornamento e/o inibendo la riproposizione di notizie risalenti nel tempo o superate da accadimenti nuovi.

[117] Cfr. art. 1 d.lgs. 196/2003. Come autorevolmente notato, in ambito europeo si assiste al consolidamento «della nozione di dignità della persona quale argine (anche) a fenomeni di stigmatizzazione sovrabbondante» (Zeno-Zencovich (2007), p. 274). Nella sterminata letteratura, sul collegamento tra «pretesa di riappropriarsi della propria storia personale» e dignità umana, Frosini (2015), p. 2; ; già prima della 'esplosione' del diritto all'oblio, sulla vicinanza tra *privacy* e dignità nel contesto continentale europeo, Resta (2010), pp. 33s. In chiave penalistica, collega la contestualizzazione dell'informazione alla tutela della dignità Piergallini (2014), p. 2377; stabilisce una correlazione tra 'pena di vergogna' e lesione della dignità Visconti (2011b), pp. 662s; più in generale, sulla *dignità* intesa come «qualificazione normativa dell'essere umano», da adoperare - con cautela e in prospettiva complementare - come contro-interesse della libertà di manifestazione del pensiero, Bacco (2013), p. 823 e bibliografia ivi contenuta.

[118] Ancor prima, parafrasando Luhmann (2002), pp. 56, 123, si potrebbe dire che le tecniche di conservazione su internet conferiscano un nuovo significato allo scarto tra ricordo e dimenticanza: «il problema che si pone quindi per il sistema delle società e che viene risolto essenzialmente con i *mass media* è il seguente: come si possono combinare la funzione di memoria e la funzione di oscillazione, se per farlo si ha a disposizione solo il presente, cioè in pratica non si ha tempo?»

[119] Nel ricco dibattito sulla criminalizzazione del negazionismo, critici sull'impiego della memoria come referente di tutela Fronza (2008), pp. 49ss; ora *amplius* Ead. (2018), part. pp. 73ss; Insolera (2018), pp. 7s, 12; Macchia (2019), p. 26. Al di fuori dell'àmbito penalistico, sulle 'trappole' insite nella giuridificazione della memoria collettiva, Pugiotto (2009), pp. 10ss.

[120] Zeno-Zencovich (2007), p. 275.

[121] De Simone (2018), p. 42. Sul problematico rapporto tra diritto penale e *fake news*, si rinvia *supra* al contributo di Costantini. In tempi meno recenti e in prospettiva più lata, sulle differenze tra violazione del diritto alla presunzione di non colpevolezza e diritto alla reputazione, Resta (2010), pp. 44s.

[122] Consolidata giurisprudenza esclude che la blanda contravvenzione che incrimina la diffusione di atti o documenti coperti da segreto (art. 684 c.p.) tuteli anche la reputazione del supposto autore del reato: «*La fattispecie criminosa di pubblicazione arbitraria di atti di un procedimento penale di cui all'art. 684 c.p. integra un reato monoffensivo, tutelando solo l'amministrazione della giustizia e non anche la reputazione e la riservatezza del soggetto sottoposto a procedimento penale posto che obiettivo della norma, prima della conclusione delle indagini preliminari, è quello di non compromettere il buon andamento delle stesse e, dopo tale momento, quello di salvaguardare i principi propri del processo accusatorio*» (Cass. civ. sez. un., sent. n. 3727/2016; conf. Cass. civ. sez. un., sent. n. 15815/2016; Cass. civ. sez. III, sent. n. 1215/2017).

a convergere: per un verso, lo 'specchio deformante' dei *mass media*[123] e la memoria infinita della rete rendono talora complicato distinguere un'informazione radicalmente falsa da, rispettivamente, un'informazione veridica distorta e un'informazione vera non contestualizzata[124]; per l'altro, sebbene giudicata espansione poco appropriata[125], il GDPR estende ora l'applicabilità del diritto all'oblio ai dati personali trattati illecitamente (art. 17 § 1 lett. *d*). Una vera e propria matassa che se, da un lato, certamente non esime dall'operare le dovute differenziazioni, dall'altro, in certi casi, probabilmente consente di non esasperarle.

L'esigenza di bilanciamento che caratterizza normalmente la dialettica oblio/informazione, nel contesto della cronaca giudiziaria penale, si fa ancora più pressante, specie laddove l'indagato rivesta un ruolo pubblico. A tal proposito, le *Linee guida* del WP 29 fissano un criterio specifico nell'eventualità che l'informazione di cui il titolare chiede la rimozione attenga alla commissione d'un reato: dando atto delle possibili divergenze legislative fra i vari Paesi, il WP 29 invita le autorità nazionali per la protezione dei dati personali a risolvere le questioni caso per caso, preferendo, rispettivamente, la de-indicizzazione dei *link* relativi a reati lievi remoti e la conservazione dei *link* relativi a reati gravi recenti (n. 13). Il criterio, in sé, appare piuttosto sterile, limitandosi il WP 29 a delineare la soluzione dei casi 'estremi' senza fare chiarezza su quelli più sfumati; in tale ultima evenienza, ad ogni modo, è possibile ricorrere agli ulteriori criteri generali, che il WP 29, come ricordato, raccomanda di combinare secondo le specificità del caso concreto.

5.1. *Sedi e rimedi. L'autoregolazione del motore di ricerca.*

L'ordinamento riconosce in capo alla vittima mediatica numerosi strumenti volti alla 'neutralizzazione' delle informazioni pregiudizievoli; strumenti, in tutta evidenza, variamente modulabili a seconda che il soggetto deduca il mancato aggiornamento di una notizia originariamente colpevolista oppure il lungo lasso temporale trascorso dopo una condanna[126]. La rete, peraltro, se, da un lato, aumenta le occasioni di aggressione alla sfera individuale, dall'altro, offre forme di tutela ulteriori, innovando quelle tradizionali o prevedendone di inedite.

Fra quest'ultime, si segnalano, in particolare, le regole messe a punto dai singoli motori di ricerca all'indomani della sentenza *Google Spain*; manovra, questa, espressamente caldeggiata dal WP 29 nelle succitate *Linee guida*. Volendoci limitare al 'diretto interessato', notiamo che, per ottemperare ai *dicta* della Corte di Giustizia, il gigante di Mountain View s'è mosso in due direzioni: creando una procedura interna attraverso cui l'interessato può chiedere la rimozione di risultati associati al proprio nome, in un senso; istituendo un apposito *Google Advisory Council* per esaminare, di concerto con numerosi soggetti di estrazione varia (governi, aziende, *media*, accademici ecc.), «questioni complesse che intercorrono tra il diritto all'informazione e il diritto alla *privacy*», nell'altro[127]. Si tratta di meccanismi certamente positivi sulla carta; a livello pratico, tuttavia, essi scontano la pressoché totale arbitrarietà della valutazione da parte del motore di ricerca, investito, come puntualmente notato, d'una pericolosa funzione 'para-costituzionale'[128] esercitata in assenza di contraddittorio.

5.1.1. Segue*: il Garante Privacy.*

In caso di rigetto o di mancato riscontro dell'istanza, l'interessato può, chiaramente, adire le vie legali ordinarie.

[123] Giostra (2016), pp. 76, 80; Id. (2018b), p. 26.
[124] La parziale sovrapposizione è dimostrata dalla possibilità che il Garante per la *privacy*, formalmente competente per questioni relative alla riservatezza, (v. *infra* § 5.1.1) accolga richieste di rimozione di *link* contenenti notizie false. Cfr. AGPDP, provv. n. 84/2016.
[125] Rugani (2018), p. 463.
[126] Manes (2017), p. 122, puntualmente sottolinea che di 'vittima mediatica' può parlarsi *anche* laddove il soggetto venga poi effettivamente condannato.
[127] Bonavita (2016), pp. 222ss; Martinelli (2017), pp. 200ss, 212ss.
[128] Pollicino (2014), a questo link. In tal senso, si è sottolineato che il rapporto di Google di poco successivo alle *Linee guida* del WP 29 appare «una contromossa *politica*, inquadrata in una strategia complessiva resa attuabile dagli ampi margini di manovra lasciati aperti dalla decisione della Corte […] Google […] non soltanto ha definito una dettagliata procedura con cui l'interessato può presentare, attraverso un apposito modulo, una richiesta nella quale devono essere indicati alcuni dati essenziali […] ma ha anche stabilito i parametri che prenderà in considerazione per valutare la richiesta» (Pietropaoli (2017), pp. 76s); critica anche Stradella (2017), p. 94.

La sede 'naturale' ove muovere le proprie rimostranze è, in tutta evidenza, l'Autorità Garante per la Protezione dei Dati Personali (AGPDP o semplicemente 'Garante'). Il quadro giuridico entro cui il Garante è chiamato ad operare si presenta notevolmente complesso e frastagliato: attualmente, esso è ricavabile dall'intreccio tra GDPR, decreti d'attuazione[129] e codice della *privacy* (d.lgs. 196/2003), fortemente rimaneggiato. Fra i suoi numerosi poteri, per quanto ci occupa, il Garante annovera quello di «*trattare i reclami presentati ai sensi del Regolamento*» (art. 154 co. 1 lett. *b* d.lgs. 196/2003, come modificato dal d.lgs. 101/2018)[130] e quello di «*assicurare la tutela dei diritti e delle libertà fondamentali degli individui dando idonea attuazione al Regolamento e al presente codice*» (art. 154 co. 1 lett. *f* d.lgs. 196/2003, come modificato dal d.lgs. 101/2018). Significativa, ai nostri fini, la previsione che, nell'adottare il proprio regolamento *ad hoc*, il Garante assicuri «*modalità semplificate e termini abbreviati per la trattazione di reclami*» che abbiano ad oggetto la violazione del diritto di rettifica, di cancellazione/oblio, di limitazione e di opposizione al trattamento (art. 142 co. 5 d.lgs. 196/2003).

Sul punto, l'approccio del Garante parrebbe divergere, per un verso, a seconda che la richiesta sia mossa contro il motore di ricerca ovvero contro l'editore del sito-fonte[131]; per l'altro, a seconda del tipo di richiesta concretamente avanzata. Nel complesso, il campionario di procedimenti intentati per chiedere rimozione, cancellazione, de-indicizzazione, contestualizzazione ecc. di (dati che incorporano) notizie relative a coinvolgimenti penali è ricco e sfaccettato, anche in considerazione del fatto che, sulla scia della sentenza *Google Spain*, gli interessati possono avanzare richieste '*a partire* dal nome', locuzione «*da intendersi inclusiva anche di ulteriori elementi di specificazione*»[132] (es., 'Tizio', 'Tizio processo', 'Tizio condanna' ecc.).

Nell'impossibilità di offrire una rassegna completa, ci limitiamo a tracciare le coordinate interpretative normalmente seguite dal Garante. Muovendosi nel solco tracciato dal WP 29, l'AGPDP effettua le proprie valutazioni soppesando il diritto alla riservatezza/identità dell'accusato, da un lato; il suo eventuale ruolo pubblico, il tempo trascorso dal processo e la natura del reato contestato, dall'altro. Come premesso, i casi di più agevole soluzione sono senz'altro quelli 'estremi'. In questo senso, a titolo d'esempio, è stata giudicata infondata la richiesta di de-indicizzazione avanzata da soggetto condannato per reati di stampo terroristico ed eversivo dell'ordine democratico durante i cc.dd. anni di piombo[133], mentre è stata accolta la richiesta di aggiornamento e de-indicizzazione d'un articolo relativo ad un procedimento archiviato appena due mesi dopo la pubblicazione[134]. Nell'area intermedia, si colloca una casistica ampia e variegata, che contempla, per restare agli esempi più vicini, casi di rigetto di richieste aventi ad oggetto procedimenti recenti[135] o addirittura in corso[136]; provvedimenti che dichiarano l'infondatezza della richiesta sulla base della 'riattualizzazione' delle informazioni di cui si chiede la rimozione[137]; provvedimenti che dichiarano l'infondatezza della richiesta in considerazione della natura del reato e del ruolo pubblico rivestito dall'interessato[138]; provvedimenti in cui viene ingiunta la sola de-indicizzazione parziale[139]; provvedimenti che

[129] Ciò che, come efficacemente detto, contribuisce a fare del Regolamento una «maxi-direttiva *in disguise*» (Bonavita - Pardolesi (2018b), p. 270).
[130] Cfr. artt. 77 ss GDPR e art. 140-*bis* ss d.lgs. 196/2003.
[131] Cfr. AGPDP, provv. n. 548/2014.
[132] AGPDP, provv. n. 277/2017.
[133] AGPDP, provv. n. 152/2016. Nel caso di specie, spiega il Garante, deve ritenersi prevalente l'interesse del pubblico ad accedere alle notizie, considerato che «*i reati di cui l'interessato si è macchiato risultano fra quelli particolarmente gravi indicati dal WP 29*» e che le relative informazioni «*riguardano una delle pagine più buie della storia italiana, della quale il ricorrente* […] *è stato* […] *un vero e proprio protagonista di spicco, ed hanno ormai assunto una valenza storica avendo segnato la memoria collettiva*».
[134] AGPDP, provv. n. 280/2017. Nel caso di specie, il Garante, dopo aver imposto la corretta contestualizzazione della notizia - che ancora faceva riferimento al procedimento senza dar conto dell'archiviazione - precisa che, alla luce del tempo trascorso, «*la perdurante diffusione delle notizie attuata attraverso l'indicizzazione dell'articolo, pur se adeguatamente aggiornato, tramite i motori di ricerca esterni al sito del quotidiano* on-line *non appare pertanto giustificabile sulla base di un supposto attuale interesse pubblico alla conoscibilità della notizia*».
[135] Cfr. AGPDP, provv. n. 344/2018; AGPDP, provv. n. 400/2016.
[136] Cfr. AGPDP, provv. n. 9/2019.
[137] Cfr. AGPDP, provv. n. 8/2019, nel quale, in relazione ad un procedimento per associazione a delinquere e violazioni fiscali nel settore dell'*import-export*, il Garante dichiara infondata la richiesta adducendo che «*le informazioni riportate all'interno degli articoli reperibili tramite gli url dei quali è stata chiesta la rimozione, pur risalenti all'epoca in cui è stata avviata l'inchiesta (2009), risultano collegate ad altri di recente pubblicazione che riprendono la notizia dando anche atto degli sviluppi giudiziari della vicenda, con particolare riguardo all'intervenuta prescrizione di parte dei reati contestati*».
[138] Cfr. AGPDP, provv. n. 9/2019, in materia di reati fiscali; AGPDP, provv. n. 505/2018, che dichiara infondata la richiesta di de-indicizzazione di articoli relativi ad una condanna definitiva per violenza sessuale aggravata commessa da soggetto successivamente divenuto avvocato; AGPDP, provv. n. 503/2018, in materia di non meglio precisati reati d'impresa, peraltro corredati dal sequestro preventivo d'una ingente somma di denaro.
[139] Cfr. AGPDP, provv. n. 260/2015, nella quale il Garante accoglie la richiesta unicamente in relazione agli url che suscitavano l'impressione

ritengono fondata la richiesta di de-indicizzazione di articoli non aggiornati[140] o parziali[141], inidonei a fornire una rappresentazione contestualizzata - e, quindi, veritiera - del soggetto interessato. Nutriti, infine, sono i casi di non luogo a provvedere per spontanea attivazione del motore di ricerca[142], dell'editore[143] o di entrambi[144]. A conferma della distinzione tra lesione della riservatezza (anche nell'accezione di 'identità dinamica') e reputazione *tout court*, ad ogni modo, fuoriescono dalla competenza del Garante le domande di tutela contro articoli contenenti mere opinioni diffamatorie[145].

5.1.2. Segue*: la via giudiziaria.*

La giurisprudenza in materia di diritto all'oblio, anche per sovraesposizione da processo penale, vede la naturale predominanza del foro civile[146]. La ragione è duplice: dal punto di vista formale, è il codice della *privacy* stesso a sancire la competenza del giudice civile per «*le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli artt. 78 e 79 del Regolamento e quelli comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali*» (artt. 143 co. 4 e 152 d.lgs. 196/2003); dal punto di vista pragmatico, poi, è assai frequente che alla tutela da vittimizzazione mediatica sia associata una richiesta di risarcimento danni[147], certamente meglio 'governabile' all'interno del giudizio civile[148]. Più in generale, possiamo affermare che il crescente ricorso all'apparato civilistico sia ampiamente motivato dalla sua maggior elasticità - e, dunque, maggior efficacia - rispetto agli strumenti penalistici[149].

Come già detto, ad ogni modo, tanto in àmbito civile quanto in àmbito penale «la tecnica di tutela usata, malgrado l'omaggio alla tradizione del linguaggio adottato, non è quella del diritto soggettivo di struttura dominicale, che si concretizza rispetto ad uno specifico bene o interesse, ma è quella di effettuare un particolare bilanciamento tra interessi protetti», entrambi di rango fondamentale[150].

(I) Negli ultimi anni, le controversie incentrate sul rapporto tra diritto all'oblio e diritto di cronaca storico-giudiziaria hanno subìto un notevole incremento[151]. Volendo tracciare due direttrici di massima, ci pare che, da un lato, l'interesse pubblico all'informazione assuma un

di un coinvolgimento diretto dell'interessato, rigettandola rispetto agli url che davano semplicemente conto della vicenda (responsabilità sanitaria nel c.d. caso del sangue infetto).

[140] Cfr. AGPDP, provv. n. 10/2019, relativo alla richiesta di de-indicizzazione avanzata da un parlamentare in relazione ad articoli su vicende risalenti nel tempo e superate da una pronuncia di assoluzione; AGPDP, provv. n. 11/2019, ove il Garante, preso atto dell'impossibilità di rimuovere l'informazione dal sito-fonte, impone al motore di ricerca la de-indicizzazione di un url che rimandava ad un articolo che non dava conto della revoca d'una misura cautelare e della richiesta d'archiviazione avanzata dal pm.

[141] Cfr. AGPDP, provv. n. 17/2019, ove il pregiudizio, argomenta il Garante, deriva dal fatto che «*le pagine reperibili tramite gli url segnalati* [consentano] *di disporre solo di dati parziali in quanto, per l'accesso alla versione completa dei predetti commenti, rinviano ad un sito, che è il medesimo per tutti i* link *individuati nell'atto di reclamo, che, allo stato attuale, risulta sospeso*».

[142] Cfr. AGPDP, provv. n. 285/2018, in relazioni ad alcuni url di cui era stata chiesta la de-indicizzazione; in AGPDP, provv. n. 506/2018, il Garante, dichiarata infondata la richiesta di de-indicizzazione, puntualizza che «*con riferimento agli url che contengono le informazioni relative alla vicenda del reclamante riportate in via incidentale e nei quali si riferiscono vicende giudiziarie che lo hanno comunque interessato, il medesimo potrebbe attivare richieste di aggiornamento ai rispettivi titolari del trattamento*».

[143] Cfr. AGPDP, provv. n. 306/2018, in relazione a numerosi fra gli editori citati.

[144] Cfr. AGPDP, provv. n. 504/2018; AGPDP, provv. n. 401/2018; AGPDP, provv. n. 21/2018.

[145] Cfr. AGPDP, provv. n. 15/2019; AGPDP, provv. n. 156/2016; AGPDP, provv. n. 54/2016. In senso meno netto, cfr. AGPDP, provv. n. 577/2017.

[146] Nel caso in cui la violazione della normativa sulla *privacy* sia dedotta per far valere la lesione di beni giuridici ulteriori rispetto alla mera riservatezza (onore, reputazione, immagine, identità personale ecc.), è competente non il foro del titolare del trattamento dei dati bensì quello di residenza dell'attore (T. Lucca, sent. n. 96/2019).

[147] Nella sua primigenia definizione, come ricordato, la pretesa d'oblio è stata ancorata al «*giusto interesse di ogni persona a non restare indeterminatamente esposta ai* danni ulteriori *che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata*» (Cass. civ. sez. III, sent. n. 3679/1998). L'entità del risarcimento va quantificata in via equitativa (Cass. civ. sez. I, sent. n. 13161/2016; in dottrina, Pisapia (2017), pp. 91s). Ad avviso di recente giurisprudenza, l'entità del risarcimento per danno morale soggettivo è diminuita in considerazione della precedente condanna comunque riportata dall'autore, che già aveva minato la reputazione di cui l'interessato godeva presso la collettività (T. Roma sez. I., sent. n. 15743/2017, in relazione ad un membro delle Forze dell'ordine condannato per falso ideologico nel processo sulla scuola Diaz di Genova).

[148] Per una ricognizione sul livello dei risarcimenti per danno da esposizione mediatica da parte del Tribunale di Milano, recentemente, Peron (2018).

[149] Resta (2010), pp. 37ss.

[150] Tucci (2010), pp. 127, 147. Per una ricostruzione teorica alternativa dell'oblio quale interesse legittimo, Vesto (2018), pp. 116ss.

[151] Per una panoramica, Pezzella (2016), pp. 885ss.

peso maggiore quando i fatti attengono a vicende criminali[152]; dall'altro, i diritti alla personalità della vittima mediatica stiano ricevendo via via maggior attenzione, anche in relazione a notizie presenti sul *web*[153].

Di grande rilievo, in quest'ultimo senso, una sentenza del 2012 resa dalla III Sezione della Cassazione. L'attore, in tempi risalenti, era stato coinvolto in un processo per corruzione, successivamente conclusosi col suo proscioglimento. In virtù dell'esito processuale e del tempo trascorso, egli chiedeva la rimozione del relativo articolo dall'archivio *online* di un noto quotidiano; tuttavia, né il Garante né il giudice dell'opposizione ritenevano di accogliere la sua richiesta. La pronuncia della Cassazione segna una tappa importante nell'evoluzione domestica del diritto all'oblio: definita la memoria di internet come un «*deposito di archivi*» ove «*le informazioni non sono in realtà organizzate e strutturate, ma risultano isolate, poste tutte al medesimo livello ('appiattite'), senza una valutazione del relativo peso*», la Corte riconosce l'esistenza di «*diritto alla tutela dinamica dei propri dati e della propria immagine sociale, che può tradursi, anche quando trattasi di notizia vera - e* a fortiori *se di cronaca - nella pretesa alla contestualizzazione e aggiornamento della notizia*»; non dare conto degli sviluppi d'una determinata vicenda giudiziaria, prosegue la Corte, rende «*la notizia, originariamente completa e vera*, […] non aggiornata, *quindi parziale e non esatta, e pertanto sostanzialmente non vera*»[154]. Affinché i requisiti di verità ed esattezza restino rispettati anche in séguito al trasferimento in archivio, dunque, è indispensabile che il titolare del trattamento - qui riconosciuto nella testata giornalistica - adotti misure che, senza arrivare alla cancellazione o alla de-indicizzazione, consentano nondimeno «*l'effettiva fruizione della notizia aggiornata*»[155].

La preminenza del diritto individuale all'oblio sul diritto del pubblico all'informazione è stata variamente confermata in successive pronunce di merito[156] e di legittimità[157]; in tali frangenti, ad uno sguardo più ampio, emerge la centralità dei princìpi generali di *attualità* e *correttezza* nel trattamento dei dati personali.

Sul punto, giova segnalare che la definizione dei criteri di bilanciamento tra diritto di cronaca e diritto all'oblio è stata ultimamente oggetto di rimessione alle Sezioni unite[158]. Nel caso specifico, l'attore si doleva della ripubblicazione *cartacea* di informazioni relative ad una condanna per omicidio emessa oltre vent'anni prima; la riproposizione di quella vicenda, pur effettuata in toni sobri e non irrispettosi, aveva provocato in lui sentimenti di profonda angoscia e prostrazione. Nello sciogliere il nodo, le Sezioni unite mutano l'angolo visuale rispetto all'ordinanza di rimessione: non già diritto di cronaca - inquadrabile nella cornice temporale entro cui un fatto si svolge o, al più, ridiventa attuale - bensì «*diritto alla rievocazione storica (storiografica)*»; attività senz'altro preziosa, si legge, ma diversa dalla prima e, perciò, non coperta dalla medesima garanzia costituzionale. Ne consegue che, quando una notizia del passato, «*a suo tempo diffusa nel legittimo esercizio del diritto di cronaca, venga ad essere nuovamente diffusa a distanza di un lasso di tempo significativo, sulla base di una libera scelta editoriale […] il diritto dell'interessato al mantenimento dell'anonimato sulla sua identità personale è prevalente, a meno che non sussista un rinnovato interesse pubblico ai fatti ovvero il protagonista abbia ricoperto o ricopra*

[152] T. Roma sez. I, sent. n. 23771/2015, che ha negato il diritto de-indicizzazione in capo a un soggetto coinvolto da inchieste sulla malavita romana, apparentemente tuttora in corso; *a contrario*, anche Cass. civ. sez. I, ord. n. 6919/2018, part. § 4.2, cui si rimanda per un interessante - sebbene discutibile - spunto sul contrasto tra diritto all'oblio e diritto di satira.

[153] In relazione ad articoli su carta stampata, Cass. civ. sez. III, sent. n. 16111/2013, che ha riconosciuto la prevalenza del diritto all'oblio sul diritto cronaca in virtù del collegamento totalmente arbitrario tra un fatto d'attualità (il ritrovamento di un arsenale di armi) e una condanna remota a carico dell'interessato (per la sua affiliazione ad un gruppo terroristico).

[154] Cass. civ. sez. III, sent. n. 5525/2012.

[155] Cass. civ. sez. III, sent. n. 5525/2012, che accoglie il ricorso imponendo «*la predisposizione di un sistema idoneo a segnalare (nel corpo o a margine) la sussistenza di un seguito e di uno sviluppo della notizia, e quale esso sia stato* […] *consentendo il rapido ed agevole accesso da parte degli utenti ai fini del relativo approfondimento*».

[156] T. Mantova, sent. 28.10.2016, che condanna un editore: *(i)* a rimuovere dall'archivio *online* un articolo riferito ad una presunta truffa contrattuale definita, nelle more, sia in sede civile che penale; *(ii)* a risarcire gli attori per il danno alla reputazione dovuto alla permanenza dell'articolo nonostante l'esplicita diffida alla rimozione avanzata tre anni prima; T. Milano sez. I, sent. n. 12623/2017, che rigetta il ricorso di un motore di ricerca avverso il provvedimento dell'AGPDP che aveva imposto la de-indicizzazione e la rimozione delle copie *cache* di numerosi url relativi a un crac finanziario mai sfociato in sentenza penale.

[157] Cass. civ. sez. I, sent. n. 13161/2016, che rigetta il ricorso di un editore ravvisando la violazione della normativa sui dati personali non già nella pubblicazione originale di un articolo relativo ad un procedimento penale, bensì «*nel mantenimento del diretto ed agevole accesso a quel risalente servizio giornalistico pubblicato il* [omissis] *e della sua diffusione sul* web *quanto meno a far tempo dal ricevimento della diffida in data* [omissis] *per la rimozione di questa pubblicazione dalla rete*». «*La persistente pubblicazione e diffusione sul sito* web *della notizia di cronaca in questione risalente al* […]», prosegue la Corte, «*appare per l'oggettiva e prevalente componente divulgativa esorbitare dal mero ambito del lecito trattamento d'archiviazione o memorizzazione* online *di dati giornalistici per scopi storici o redazionali*».

[158] Cass. civ. sez. III, ord. n. 28084/2018, con osservazioni di Febbrajo (2019) e di Di Ciommo (2019), il quale, peraltro, avanza qualche dubbio circa la ritualità della rimessione (*op. ult. cit.*, p. 9).

una funzione che lo renda pubblicamente noto»[159]. Consapevole delle peculiarità del caso concreto, la Corte restringe il campo d'indagine alla sola ripubblicazione su carta; ad ogni modo, sebbene non direttamente riferibile all'archiviazione *online*, è immaginabile che detto principio costituirà un importante punto di riferimento *anche* per il regime applicabile agli articoli di cronaca 'conservati' su internet, ove, ricorrendone i presupposti, la pretesa di anonimizzazione vanta ragioni ancora più solide[160].

(II) Di contro, la giurisprudenza penale appare di minor consistenza e, comunque, riferibile a canali mediatici diversi da internet, come giornali, libri e *talk-show*. In prospettiva criminale, l'oblio è intimamente legato al delitto di diffamazione[161]; i percorsi argomentativi battuti per valorizzarlo sono essenzialmente due.

In un primo senso, è possibile sfruttare l'elemento temporale alla base della tutela dell'identità dinamica per orientare in senso diacronico due dei criteri tradizionalmente impiegati per dirimere il contrasto tra tutela della reputazione e diritto all'informazione: *verità* e *pertinenza*. In quest'ottica, ad esempio, si è affermato che, nell'àmbito dell'attività di ricostruzione storica, l'esposizione di fatti distanti nel tempo impone al redattore obblighi più stringenti di verifica delle fonti[162].

In senso diverso - sebbene, tutto sommato, affine - è invece possibile ritenere l'identità dinamica un profilo peculiare e autonomamente aggredibile del bene 'reputazione'. In questa direzione, milita una pionieristica sentenza della Cassazione d'una decina di anni fa[163]. Nel confermare la sentenza di condanna per diffamazione, il Collegio, oltre al difetto di verità e attualità della notizia, rileva la violazione *autonoma* del diritto all'oblio delle persone offese: «*Riferire, a distanza di tempo, dello sviluppo di indagini di polizia giudiziaria*», si argomenta, «*deve ritenersi consentito in una ricostruzione storica dell'evento, pure a distanza di tempo e persino in chiave di critica all'operato degli inquirenti ed al modo in cui è stata svolta l'inchiesta* […] *Ma in tali casi l'obbligo deontologico del giornalista deve parametrarsi a criteri di rigore ancora maggiore dell'ordinario. Non gli è, infatti, consentito, neppure in chiave retrospettiva, riferire di ipotesi investigative o di meri sospetti degli inquirenti (veri o presunti che siano) senza precisare, al tempo stesso, che quelle ipotesi o sospetti sono rimasti privi di riscontro* […] *Ove esigenze di ricostruzione storica od artistica lo richiedano e permanga – o si riattualizzi – l'interesse pubblico alla relativa propalazione, la notizia deve essere accompagnata dalla doverosa avvertenza che le tesi investigative sono rimaste a livello di mera ipotesi di lavoro in quanto non hanno trovato alcuna conferma o, addirittura, sono state decisamente smentite dallo sviluppo istruttorio* […] *Una notizia monca od incompleta è capace, infatti, di ledere l'onorabilità dell'interessato e la proiezione sociale della sua personalità*».

L'esiguità della casistica e la coesistenza di decisioni di segno diverso[164] rendono prematuro, allo stato attuale, il tentativo di individuare *trend* unitari; le sinergie e le contaminazioni tra civile e penale che caratterizzano quest'epoca[165], ad ogni modo, lasciano presagire sviluppi anche in questo particolare frangente[166].

[159] Cass. civ. sez. un., sent. n. 19681/2019.

[160] In tal senso, si considerino anche i ripetuti richiami a Cass. civ. sez. III, sent. n. 5525/2012. Peraltro, valorizzando il reinserimento sociale dell'attore in séguito all'espiazione della pena (v. *supra* n. 108), la sentenza sembra farsi parzialmente carico dell'esigenza, puntualmente segnalata in dottrina [Febbrajo (2019)], di differenziare il bilanciamento a seconda che la notizia riguardi o meno vicende penalmente rilevanti.

[161] Quanto alle rare ipotesi diverse, s'è ritenuto, ad esempio, che la divulgazione di notizie relative a vecchi procedimenti disciplinari a carico di un magistrato - ottenute e propalate in spregio delle norme regolamentari del CSM - possa rappresentare il 'danno ingiusto' elemento costitutivo *ex* art. 323 c.p. (Cass. pen. sez. VI, sent. n. 39452/2016.) In prospettiva opposta, da ultimo, la Cassazione ha statuito che l'erroneo convincimento di poter esercitare il diritto all'oblio esclude il dolo di calunnia (Cass. pen. sez. VI, sent. n. 17112/2019).

[162] Cass. pen. sez. I, sent. 13941/2015, relativa alla pubblicazione di un libro sulla criminalità organizzata con richiami non aggiornati alla posizione della persona offesa.

[163] Cass. pen. sez. V, sent. n. 45051/2009. Il caso riguardava la messa in onda d'un servizio relativo ad un fatto di cronaca nera; detto servizio, stando alle contestazioni, veniva condotto in maniera parziale, lacunosa e allusiva, facendo generoso ricorso a mere congetture platealmente smentite dal corso degli eventi.

[164] Ad es., la riesumazione giornalistica d'una vecchia vicenda giudiziaria che aveva coinvolto un esponente di casa Savoia è stata giudicata in linea con l'interesse pubblico e, perciò, pienamente scriminata (Cass. pen. sez. V, sent. n. 38747/2017).

[165] Piergallini (2012), pp. 121ss.

[166] In senso inverso, sono le stesse Sezioni unite civili a stimare rilevanti i contributi provenienti dalla giurisprudenza penale (cfr. ancora Cass. civ. sez. un., sent. n. 19681/2019).

5.2. *Un diritto* umano *all'oblio? Resistenze e prospettive nella giurisprudenza CEDU.*

Un accenno rapido merita, infine, la giurisprudenza della Corte Europea dei Diritti dell'Uomo (Corte EDU); come acutamente evidenziato, difatti, muovendo dalla dottrina dei cc.dd. obblighi positivi, è possibile ipotizzare in capo allo Stato doveri di protezione *pure* verso la vittima mediatica[167].

Anche nel *case-law* di Strasburgo, il tema memoria/oblio s'insinua nell'intricato rapporto tra libertà d'espressione (art. 10 CEDU) e diritto al rispetto della vita privata (art. 8 CEDU); rapporto che, considerato lo storico impegno della Corte nell'adeguare le norme convenzionali alle nuove tecnologie[168], con l'avvento di internet ha subìto significative mutazioni[169].

In via generale, la Corte EDU è solita ribadire che i princìpi elaborati per dirimere il contrasto tra i due diritti meritano eguale ponderazione, a prescindere che il ricorrente invochi la violazione dell'uno (es., il giornalista che si duole della sanzione sproporzionata per un articolo diffamatorio) o dell'altro (es., il privato che si duole della conservazione d'un articolo dai contenuti diffamatori). I criteri-guida, successivamente mutuati dalle corti nazionali, sono frutto di giurisprudenza ormai stratificata e riguardano: *(i)* il contributo a un dibattito di pubblico interesse e la notorietà della persona coinvolta; *(ii)* la precedente condotta del soggetto; *(iii)* il modo in cui chi diffonde la notizia è venuto in possesso delle informazioni; *(iv)* il contenuto, la forma e la conseguenze della pubblicazione; *(v)* le circostanze in cui la notizia è stata diffusa[170].

Ad avviso della dottrina, nel passaggio al virtuale, la Corte ha rimodulato la portata che l'art. 10 CEDU aveva assunto in ambiente analogico, ritenendo «verosimile che il mezzo [internet] generi pericolo per gli altri diritti» e assumendo, perciò, «la necessità, e quindi la legittimità di correttivi che possano limitare l'esercizio del *free speech*»[171]. Sennonché, al momento, tale considerazione parrebbe trovare nel diritto all'oblio una vistosa eccezione: pur avendo esplicitamente riconosciuto il problema della permanenza *online* di contenuti lesivi della reputazione[172], infatti, la Corte ha finora preferito, per così dire, dimenticarsi del diritto a essere dimenticati[173], soprattutto quando l'informazione che si vorrebbe accantonata attenga a responsabilità penali[174]. Significativa, in tal senso, l'assenza di qualsivoglia riferimento al decorso temporale tra i fattori da prendere in considerazione ai fini del bilanciamento.

Ad ogni modo, mentre verso l'oblio *stricto sensu* la Corte mostra un atteggiamento di netta chiusura, maggiore sensibilità si registra rispetto alle istanze di corretta contestualizzazione: nel negare la violazione CEDU per via della permanenza in rete di contenuti lesivi, in effetti, i giudici di Strasburgo prendono espressamente in considerazione le misure adottate a livello nazionale a tutela dell'identità personale dei ricorrenti, come l'aggiornamento della notizia[175] o, quantomeno, la sua archiviazione in una sezione del sito appositamente dedicata alle vicende storiche[176]. In aggiunta, a quanto ci consta, la Corte non ha ancora avuto modo di giudicare ricorsi sorti a causa d'un rigetto di de-indicizzazione[177]; in un'occasione, anzi, essa ha

[167] Manes (2017), pp. 118ss.
[168] Murphy e Ó Cuinn, (2010) p. 601, part. 617ss per quanto riguarda l'art. 8 CEDU.
[169] Sulle differenze tra *media* classici e internet, Corte EDU, *Editorial Board of Pravoye Delo and Shtekel c. Ucraina*, 5.8.2011, ric. n. 33014/05, § 63. Per una ricognizione generale sulla giurisprudenza EDU connessa a internet, si veda l'utile guida *Internet: case-law of the European Court of the Human Rights*, elaborata dalla Divisione Ricerca della Corte medesima, disponibile a questo, aggiornata al giugno 2015, disponibile a questo link.
[170] In rilievo, Corte EDU (G.C.), *Von Hannover c. Germania (2)*, 7.2.2012, ric. nn. 40660/08 e 60641/08, §§ 108ss; Corte EDU (G.C.), *Axel Springer AG*, cit., §§ 89ss; Corte EDU (G.C.), *Couderc e Hachette Filippachi Associés c. Francia*, 10.11.2015, ric. n. 40454/07, §§ 90ss.
[171] Pollicino (2018), p. 55.
[172] Corte EDU (G.C.), *Delfi AS c. Estonia*, 16.6.2015, ric. n. 64569/09, § 110.
[173] In tema, Corte EDU, *Wegryznowski e Smolczewski c. Polonia*, 16.7.2013, ric. n. 33846/07, §§ 53ss, che nega la violazione dell'art. 8 CEDU invocata per la mancata rimozione di un articolo dall'archivio *online* di un quotidiano, sottolineando che «*non spetta all'autorità giudiziaria impegnarsi a riscrivere la storia ordinando che siano sottratte dal pubblico dominio tutte le tracce di pubblicazioni rinvenibili nel passato*» (§ 65); Corte EDU, *Fuchsmann c. Germania*, 19.10.2017, ric. n. 71233, § 30ss, che nega la violazione dell'art. 8 CEDU invocata per la mancata rimozione di un articolo che adduceva sospetti su passati coinvolgimenti criminali del ricorrente, ritenendo che non sussistano «*forti ragioni*» tali da sovvertire il bilanciamento tra diritto della personalità e diritto all'informazione effettuato dalle corti nazionali (§ 54); Corte EDU, *M.L. e W.W. c. Germania*, 28.6.2018, ric. nn. 60798 e 65559/10, §§ 86ss, che nega la violazione dell'art. 8 CEDU invocata per la mancata rimozione da tre archivi *web* di informazioni relative al processo per l'omicidio dell'attore Walter Sedlmayr.
[174] Corte EDU, *M.L. e W.W. c. Germania*, cit., §§ 88, 98ss, part. 106, ove si nega che pure la mancata anonimizzazione, di per sé, integri una violazione dell'art. 8 CEDU.
[175] Corte EDU, *Wegryznowski e Smolczewski c. Polonia*, cit., § 66.
[176] Corte EDU, *M.L. e W.W. c. Germania*, cit., §§ 23, 40.
[177] Significativa, in tal senso, la statuizione contenuta in Corte EDU, *M.L. e W.W. c. Germania*, cit., § 97, ove la Corte ammette che, in

esplicitamente 'rimproverato' al ricorrente d'aver dedotto la presenza di informazioni pregiudizievoli senza aver dato prova d'essersi previamente rivolto al motore di ricerca per ottenere il *de-listing*[178].

In definitiva, a dispetto della (scarna) casistica sin qui maturata, crediamo che, sfruttando l'ampiezza semantica che il diritto all'oblio ha progressivamente assunto[179], in virtù dell'esplicito riconoscimento del «*diritto all'autodeterminazione informativa*»[180], residui la possibilità d'una sua valorizzazione anche in seno alla Corte EDU[181]. Una maggiore tutela dell'interesse «*a non doversi più confrontare col proprio atto in vista della reintegrazione in società*»[182], del resto, parrebbe porsi in sintonia col parallelo riconoscimento, in capo allo Stato, dell'obbligo positivo di risocializzazione del reo[183].

6. Stigma penale e libertà d'informazione nell'epoca di internet: un finale aperto.

Le parole di due maestri del diritto civile aiutano a tracciare le estremità del campo concettuale entro cui prende forma lo scontro tra oblio e informazione: a un capo, «l'idiosincrasia personale e l'auto-indulgenza», intese come aspirazione dell'interessato a costruire la propria immagine sociale sulla base di sole 'biografie disinfettate'[184]; all'altro, il rischio di essere condannato «a divenire ostaggio della memoria collettiva, prigionier[o] di un passato destinato a non passare mai»[185].

Osservata dall'angolo visuale della vittima mediatica, la dignità personale connessa al fluire del tempo sembra godere d'un ampio ventaglio di strumenti di tutela, spesso sovrapponibili e non ben coordinati ma comunque variamente declinabili ed esperibili in diverse sedi. La preferenza per la via Garante-giudice civile, oltretutto, limita il rischio - non infrequente - di rispondere al penale con *più* penale. È evidente, tuttavia, che tali strumenti, nell'ottica del pieno rispetto dei diritti della persona, non possono bastare: tralasciando il rischio di riacutizzazione del 'paradosso dell'oblio'[186]- ossia dare *nuova* visibilità al soggetto che, all'opposto, ne chiede il ridimensionamento[187] - infatti, essi si risolvono pur sempre in rimedi *ex-post*, attivati a lesione già consumata e protratta.

A tale ultimo proposito, evidenzia nitidamente Rodotà, la «possibilità di esercitare un controllo 'in uscita' sui dati personali deve essere accompagnata da un potere di selezione di quelli 'in entrata'»[188]. È però scontato precisare che, nel settore della cronaca giudiziaria, tale controllo 'in entrata' non possa passare dal previo consenso dell'interessato; più logico, semmai, pretendere un'inversione di rotta nella narrazione mediatica del crimine, che ristabilisca il necessario equilibrio tra il diritto pubblico d'accesso alla giustizia e il diritto individuale al rispetto della dignità. In tale ottica, appaiono certamente positivi i recenti sforzi autoregolativi

considerazione dell'effetto amplificatore del motore di ricerca, le obbligazioni in capo a quest'ultimo - e, quindi, i conseguenti profili di responsabilità in caso di mancata attivazione - possono divergere notevolmente da quelle in capo all'editore del sito che ospita la notizia.

[178] Corte EDU, *Fuchsmann c. Germania*, cit., § 53.

[179] Per qualche spunto sul possibile gioco di sponda tra CEDU e diritto UE, sia consentito il rinvio a Mazzanti (2018), part. pp. 384ss.

[180] Corte EDU, *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia*, 27.6.2017, ric. n. 913/2013, § 137.

[181] L'attenzione alla nuova 'anima' del diritto all'oblio parrebbe dimostrata dalla Raccomandazione del Consiglio d'Europa sulla protezione dei diritti umani in relazione ai motori di ricerca, adottata, peraltro, due anni prima della sentenza *Google Spain* (Recommendation CM/REC (2012)3 of the Committee of the Ministers to Member States, *On the Protection of Human Rights with Regard to Search Engines*, 4 aprile 2012, part. nn. 5ss). Segnalano il silenzio della Corte in relazione a nuove declinazioni del diritto all'oblio, pur valutando in modo critico un suo ipotetico accoglimento in seno a Strasburgo, Bonavita e Pardolesi (2018a), pp. 154s.

[182] Corte EDU, *M.L. e W.W. c. Germania*, cit., § 100.

[183] Corte EDU, *Murray c. Paesi Bassi*, 26.4.2016, ric. n. 10511/10, § 104. Sulle implicazioni di tale riconoscimento, con particolare riferimento ai condannati all'ergastolo, Meijer (2017), pp. 159ss.

[184] Pardolesi (2017), p. 79.

[185] Rodotà (2006), p. 64.

[186] Miniussi (2015), pp. 233s.

[187] Rischi del genere possono essere, se non aggirati, quantomeno limitati mediante procedure come l'anonimizzazione o la pseudonimizzazione; procedure che, in tutta evidenza, tanto più possono rivelarsi efficaci, quanto meno l'istante o anche solo la vicenda concreta siano note al grande pubblico.

[188] Rodotà (2006), p. 65.

compiuti da giornalisti[189] e magistrati[190]. Degni d'interesse, per quel che ci riguarda, sono poi i vari disegni di legge di riforma dei reati d'opinione via internet: il recente d.d.l. Verini, ad esempio, raccogliendo l'eredità della scorsa legislatura, aspira ad una sostanziosa rimodulazione della disciplina, tesa a coniugare «*il dovere di raccontare* [e] *il diritto a non essere vittima di una macchina del fango*»; significativo, in questa direzione, l'ampliamento degli obblighi di rettifica in ambiente telematico[191]. Passi importanti, dunque, ancorché, in tutta evidenza, non risolutivi, poiché destinati a lasciare inevitabilmente scoperte alcune aree (es., la diffusione di notizie tramite testate non registrate o, comunque, piattaforme 'non professioniste') e perché bisognosi d'essere affiancati, simmetricamente, da percorsi di autentica 'educazione alla legge' volti ad aumentare la consapevolezza dei fruitori-cittadini[192].

Questo il quadro, è lecito confidare in miglioramenti nel prossimo futuro? Sia consentito, purtroppo, nutrire dubbi al riguardo. Il diritto penale del nuovo millennio, solcato da logiche *fuzzy*[193], ha trovato nei *mass media* la propria *sedes materiæ*[194]: liberato da qualunque regola[195], il 'formante mediatico'[196] ha così via via preso il sopravvento, innescando un *trend* di vistoso scadimento qualitativo della rappresentazione giudiziaria. Tante e forti le grida di denuncia da parte di studiosi e operatori, tutte intente a segnalare l'urgenza di riallineamento tra *media* e strumento penale. Il modo in cui quest'istanza è stata presa in carico dalle istituzioni ha, però, del paradossale: alcune fra le più recenti riforme legislative, in effetti, riavvicinano sì sistema mediatico e sistema penale, incredibilmente modellando, però, il secondo a misura del primo. Bastino, in tal senso, un paio d'esempi tratti dall'ultima l. 3/2019[197] che, con la riforma delle pene accessorie per i delitti contro la P.A., recepisce l'istanza di moralizzazione del tessuto sociale mediante lo stigma punitivo[198]; mentre, rivoluzionando il regime di sospensione della prescrizione, lascia l'imputato in balìa d'un giudizio potenzialmente infinito[199]. Come aspettarsi maggior attenzione ai diritti dei soggetti *virtualmente* esposti, allora, se persino il sistema penale *reale* rischia di replicare i tratti di stigmatizzazione e di perpetuità tipici del 'processo un internet'?

Le criticità attuali e le grigie prospettive, in ogni caso, non devono trattenere dall'auspicare un deciso cambio di passo dell'informazione giudiziaria: come sottolineato da uno dei

[189] Si pensi al c.d. Testo unico dei doveri del giornalista, approvato dal CNS nel gennaio del 2016, e in particolare gli art. 3 (*Identità personale e diritto all'oblio*), 8 (*Cronaca giudiziaria e processi in tv*) e 9 (*Doveri in tema di rettifica e di rispetto delle fonti*). Rilevante, ai nostri fini, anche il *Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica,* allegato al predetto Testo unico. Sui pregi e i limiti dell'autoregolazione in àmbito giornalistico, Turchetti (2017), pp. 103s.

[190] Alludiamo alle *Linee guida per l'organizzazione degli uffici giudiziari ai fini di una corretta comunicazione istituzionale*, adottate dal CSM nel luglio 2018. Il documento, come autorevolmente spiegato, mira a superare le criticità e le manifestazioni di autoreferenzialità registrate in passato in seno alla magistratura, mediante una politica comunicativa, al contempo, *proattiva* e *reattiva* (Canzio, (2018), p. 1538). Interessante, ai nostri fini, il punto relativo alla 'notizia di decisione', una sorta di *abstract* «da redigere contestualmente o immediatamente dopo la deliberazione/ decisione» così da contribuire «a restringere la forbice fra quel rito (e la 'gogna' che talora ne consegue senza rimedio alcuno per il malcapitato) e il contesto spazio-temporale del giusto processo penale» (*op. ult. cit.,* p. 1540).

[191] Cfr. art. 2 AC-416, presentato alla Camera il 27.3.2018. Più di recente, art. 1 AS-812 (d.d.l. Caliendo), presentato al Senato il 20.9.2018. Con riferimento all'obbligo di rettifica, De Simone (2018), pp. 15s. Sul parallelo tra diritto di rettifica e diritto di contestualizzazione, già, Cass. civ. sez. III, sent. n. 5525/2012. Per un esame degli interventi legislativi in materia di libertà d'espressione approvati o proposti durante la precedente legislatura, Monti (2018), pp. 1ss, part. p. 17, con una critica alla proposta sull'obbligo di rettifica per come previsto nell'AS-2688 (c.d. d.d.l. Gambaro).

[192] Come insegna la migliore dottrina, si registra «una perdita di efficacia politico-criminale allorché il diritto penale sia considerato isolatamente dalle altre forme di controllo sociale» (Paliero (1990), p. 513). In ambiente virtuale, ad ogni modo, detti processi educativi sono complicati da quello che gli specialisti definiscono fenomeno c.d. della *filter bubble*, che descrive la tendenza di motori di ricerca e *social network* a proporre all'utente contenuti sempre più in linea coi propri interessi e con le proprie opinioni. Sul punto, Pitruzzella (2018), pp. 28s, 41s.

[193] Caratteristica che, per l'appunto, ne agevola la consegna al governo dei giudici, secondo «cadenze 'giursrealistiche', orientate sul caso», in forza delle quali «il diritto sta *dopo* il fatto» (Piergallini (2015), p. 262); in senso analogamente problematico, Paliero (2014), pp. 1130s.

[194] Fondaroli (2014), pp. 135, 144s, ravvisa nell'intreccio tra diritto penale casistico e spettacolarizzazione della giustizia le trame di un nuovo particolarismo giuridico; uno spunto in tal senso, anche in Giostra (2018a), p. 15.

[195] Sulla contrapposizione tra il sistema chiuso/formalizzato tipico del processo penale e il sistema aperto/informale tipico del processo mediatico, Giostra (2007), p. 59; Paliero (2006), p. 492; Conti (2016) pp. 7, 10.

[196] Paliero (2012), p. 116.

[197] In via generale e con toni fortemente critici, Manes (2019), che parla di un 'diritto penale no-limits' «che non è solo frutto di un *trade-off* tra efficienza e garanzie con un saldo conclusivo a tutto scapito di queste, ma che è un modello *altro* di diritto penale, predisposto e proteso a soddisfare pretese punitive opportunisticamente fomentate e drammatizzate, ed a realizzare – persino – una sorta di *class action* punitiva» (corsivi nell'originale).

[198] Palazzo (2019), p. 8.

[199] Per una sintesi dei principali profili di dubbia legittimità costituzionale della nuova disciplina, Pecchioni (2019), pp. 4s. Per aver conto della fervida disputa sviluppatasi intorno all'ultima riforma sfociata nella l. 3/2019, rinviamo ai contributi consultabili sul sito *Diritto penale contemporaneo* digitando la parola 'prescrizione' nella stringa di ricerca. Si consideri che il progetto, ancor prima della definitiva approvazione, ha suscitato una forte ondata di dissenso, testimoniata dal clamoroso appello al Presidente della Repubblica da parte dell'UCPI e di oltre cento professori di diritto penale e diritto costituzionale (link).

più autorevoli e ferventi critici del processo mediatico, infatti, l'accesso dell'opinione pubblica alla giustizia penale «non si pone in termini di opportunità, ma di necessità politica: per un ordinamento democratico moderno, prima ancora che essere utile una giustizia pubblica, è inconcepibile una giustizia segreta […] Sarebbe quindi costituzionalmente, politicamente e culturalmente inammissibile oscurare la cronaca giudiziaria»; nell'impossibilità di approntare rimedi definitivi, la sfida, «realisticamente difficile e democraticamente imprescindibile», è dunque quella di «indicare le condizioni in grado di favorire il maturare di un'informazione giudiziaria all'altezza della sua importantissima funzione»[200]. Con la consapevolezza che, trascinata sul terreno ruvido e viscoso del crimine, la libertà d'informazione ai tempi di internet sconta le contraddizioni della sua natura ambivalente: da un lato, la rappresentazione della giustizia 'per *screenshot*' - immediata, non ponderata e decisamente suggestiva - rischia di minare non soltanto la dignità personale dei soggetti coinvolti, ma pure le basi fondanti della democrazia[201]; dall'altro, quella stessa libertà d'informazione, ben esercitata, si appalesa sempre più indispensabile in un Paese che pare star smarrendo la memoria e in cui le attuali contingenze storico-politiche accentuano l'urgenza di adeguati contropoteri.

Bibliografia

Aa. Vv. (1996): 'Pubblicità del processo e giustizia spettacolo', in De Cataldo Neuburger (eds.): Mass media, *violenza e giustizia spettacolo* (Padova, Cedam), pp. 193-268.

Aa. Vv. (2015): *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Resta e Zeno-Zencovich (eds.) (Roma TrE-Press).

Aa. Vv. (2016): 'Il burocrate creativo. La crescente intraprendenza creativa della giurisprudenza penale', Giunta (eds.): *Criminalia*, pp. 157-254.

Accinni, Giovanni Paolo (2018): *Civiltà giuridica della comunicazione* (Milano, Giuffrè).

Agnino, Francesco (2018): 'Il diritto all'oblio e diritto all'informazione: quali condizioni per il dialogo?', *Danno e responsabilità*, 1, pp. 104-120.

Amodio, Ennio (2016): *Estetica della giustizia penale* (Milano, Giuffrè).

Aprati, Roberta (2017): 'Riflessioni intorno alla 'vittima del processo'', *Cassazione penale*, 3, pp. 977-982.

Bacco, Federico (2013): 'Dalla dignità all'eguale rispetto: libertà di espressione e limiti penalistici', *Quaderni costituzionali*, 4, pp. 823-848.

Barberio, Raffaele (2018): 'Parliamo di Russia, ma la vera anomalia sul 'data retention' è l'Italia', consultabile sul sito de *Il Fatto quotidiano* a questo link.

Bartoli, Roberto (2017): 'Tutela penale del segreto processuale e informazione: per un controllo democratico sul potere giudiziario', *Diritto penale contemporaneo – Rivista trimestrale*, 3, pp. 59-77.

Bertolino, Marta (2003): 'Privato e pubblico nella rappresentazione mediatica del reato', *Rivista italiana di diritto e procedura penale*, 4, pp. 1070-1114.

Bertolino, Marta (2012): 'Giustizia narrata o giustizia tradita?', in Forti, Mazzucato, Visconti (eds.): *Giustizia e letteratura. Volume I* (Milano, Vita e Pensiero), pp. 610-634.

Bianchetti, Raffaele (2018): *La paura del crimine* (Milano, Giuffrè).

[200] Giostra (2018a), pp. 3, 15, 10.
[201] Bianchetti (2018), pp. 506ss; Giostra (2018b), pp. 37s; Palazzo (2018), pp. 16, 18, 21. In prospettiva costituzionalistica, per una riflessione sui valori della democrazia e della libertà d'espressione/informazione in tempi di internet, Frosini (2017), pp. 662ss; Pitruzzella (2018), p. 20, part. pp. 44ss.

Bonavita, Simone (2016): *Il diritto all'oblio e la gestione delle informazioni della società iperconnessa*, tesi di dottorato, disponibile a questo link.

Bonavita, Simone e Pardolesi, Roberto (2018a): 'La Corte EDU contro il diritto all'oblio?', *Danno e responsabilità*, 2, pp. 149-155.

Bonavita, Simone e Pardolesi, Roberto (2018b): 'GDPR e diritto alla cancellazione (oblio)', *Danno e responsabilità*, 3, pp. 269-281.

Caggiano, Giandonato (2018): 'Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione', *Rivista di diritto dei media*, 2, pp. 64-82.

Canepa, Marco e Ponton, Douglas Mark (2019): 'Fair Trail in the Digital Era. English and Italian standpoint', *Rivista di diritto dei media*, 1, pp. 1-11.

Canzio, Giovanni (2017): 'Intervento del Primo Presidente Dott. Giovanni Canzio per la cerimonia di inaugurazione dell'anno giudiziario 2017', disponibile a questo link.

Canzio, Giovanni (2018): 'Un'efficace strategia comunicativa degli uffici giudiziari *vs.* il processo mediatico', *Diritto penale e processo*, 12, pp. 1537-1540.

Castells, Manuel (2002): *La nascita della società in rete*, trad. it. di Turchet (Milano, Università Bocconi Editore).

Catenacci, Mauro (2015): 'I delitti contro l'ambiente fra aspettative e realtà', *Diritto penale e processo*, 9, pp. 1073-1079.

Caterini, Mario (2013): 'Criminalità, politica e *mass media*', *Politica del diritto*, 4, pp. 601-623.

Conti, Carlotta (2016): 'La verità processuale nell'era 'post-Franzese': rappresentazioni mediatiche e scienza del dubbio', in Conti (ed.): *Processo penale e processo mediatico* (Milano, Giuffrè), pp. 1-21.

Coppola, Fabio (2018): 'Il difficile ruolo del giudice penale contemporaneo verso la prevedibile interpretazione della fattispecie', *Diritto penale e processo*, 12, pp. 1637-1647.

Cracco, Giovanna (2011-2012): 'Dalle intercettazioni alla diagnosi di un mostro', *PaginaUno*, 25, pp. 14-22.

Cuffaro, Vincenzo (2019): 'Cancellare i dati personali: dalla *damnatio memoriæ* al diritto all'oblio', disponibile a questo link, pp. 1-12 del dattiloscritto.

De Simone, Federica (2018): "*Fake news*', '*post truth*', '*hate speech*': nuovi fenomeni sociali alla prova del diritto penale', *Archivio penale*, 1, pp. 1-49.

Di Ciommo, Francesco (2017): 'Privacy in Europe after Regulation (EU) n. 679/2016: What Will Remain of the Right to Be Forgotten?', *The Italian Law Journal*, 2, pp. 623-646.

Di Ciommo, Francesco (2019): 'Oblio e cronaca: rimessa alle Sezioni unite la definizione dei criteri di bilanciamento', *Corriere giuridico*, 1, pp. 5-15.

Falcinelli, Daniela (2011): *Il tempo del reato, il reato nel tempo* (Torino, Giappichelli).

Febbrajo, Tommaso (2019): 'Il difficile bilanciamento tra diritto di cronaca e diritto all'oblio al vaglio delle Sezioni unite', *Diritto civile contemporaneo*.

Ferola, Laura (2012): 'Dal diritto all'oblio al diritto alla memoria sul *web*. L'esperienza applicativa italiana', *Diritto dell'informatica*, 6, pp. 1001-1031.

Ferrarella, Luigi (2017): Il 'giro della morte': il giornalismo giudiziario tra prassi e norme, *Diritto penale contemporaneo – Rivista trimestrale*, 3, pp. 4-19.

Finocchiaro, Giusella (2015): 'Il diritto all'oblio nel quadro dei diritti della personalità', in Resta e Zeno-Zencovich (eds.): *Il diritto all'oblio su internet dopo la sentenza Google Spain* (Roma TrE-Press), pp. 29-42.

Flor, Roberto (2015): 'La giustizia penale nella rete? Tutela della riservatezza *versus* interesse all'accertamento e alla prevenzione dei reati nella recente giurisprudenza della Corte di Giustizia dell'Unione europea', in Flor, Falcinelli, Marcolini (eds.): *La giustizia penale 'nella rete'. Le nuove sfide della società dell'informazione nell'epoca di Internet*, pp. 153-168, disponibile a questo link.

Flor, Roberto (2017): '*Data retention* e art. 132 cod. *privacy*: *vexata quæstio*(?)', *Diritto penale contemporaneo*, n. 3, pp. 356-364.

Fondaroli, Désirée (2014): 'L'accertamento della responsabilità penale secondo il paradigma del 'caso per caso' ed il 'circo mediatico-giudiziario'. Il nuovo particolarismo giuridico', *Archivio penale*, 1, pp. 135-146.

Formici, Giulia (2018): 'Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia *Ministerio Fiscal*', *Osservatorio costituzionale*, 3, pp. 453-476.

Forza, Antonio, Menegon, Giulia, Rumiati, Rino (2017): *Il giudice emotivo* (Bologna, Il Mulino).

Foucault, Michel (1993): *Sorvegliare e punire. Nascita della prigione*, trad. it. di Tarchetti (Torino, Einaudi).

Fronza, Emanuela (2008): 'Il reato di negazionismo e la protezione penale della memoria', *Ragion pratica*, 1, pp. 27-54.

Fronza, Emanuela (2018): *Memory and Punishment. Historical Denialism, Free Speech and the Limits of Criminal Law*, (The Hague - Berlin - Heidelberg, Springer).

Frosini, Tommaso Edoardo (2012): 'Il diritto all'oblio e la libertà informatica', in *Diritto dell'informatica*, 4/5, pp. 911-920.

Frosini, Tommaso Edoardo (2015): 'Google e il diritto all'oblio preso sul serio', in Resta e Zeno-Zencovich (eds.): *Il diritto all'oblio su internet dopo la sentenza Google Spain* (Roma TrE-Press), pp. 1-5.

Frosini, Tommaso Edoardo (2017): 'Internet e democrazia', *Diritto dell'informazione e dell'informatica*, 4/5, pp. 657-671.

Gargani, Alberto (2017): 'Crisi del diritto sostanziale e *vis expansiva* del processo', *Studi senesi*, pp. 59-86.

Giostra, Glauco (2007): 'Processo penale e *mass media*', *Criminalia*, pp. 57-69.

Giostra, Glauco (2016): 'L'informazione giudiziaria non soltanto distorce la realtà giudiziaria, ma la cambia', in UCPI (eds.): *L'informazione giudiziaria in Italia. Libro bianco sui rapporti tra mezzi di comunicazione e processo penale* (Pisa, Pacini), pp. 75-84.

Giostra, Glauco (2018a): 'Riflessi della rappresentazione mediatica sulla giustizia 'reale' e sulla giustizia 'percepita'', legislazionepenale.eu, 9, pp. 1-15.

Giostra, Glauco (2018b): 'La giustizia penale nello specchio deformante della cronaca giudiziaria', *Rivista di diritto dei media*, 3, pp. 23-38.

Giunta, Fausto e Micheletti, Dario (2003): Tempori cedere. *Prescrizione del reato e funzioni della pena nello scenario della ragionevole durata del processo* (Torino, Giappichelli).

Hassemer, Winfried (2004): 'Il diritto penale attraverso i *media*: messa in scena della realtà?', *Ars interpretandi. Annuario di ermeneutica giuridica*, pp. 147-194.

Insolera, Gaetano (2018): 'Tempo, memoria e diritto penale. Quale memoria per quale diritto penale?', *Diritto penale contemporaneo*, pp. 1-12.

Korenhof, Paulan e Al. (2014): 'Timing the Right to be Forgotten. A study into 'Time' as a Factor in Deciding about Retention or Erasure of Data', *working paper*, disponibile a questo link.

Loporcaro, Michele (2005): *Cattive notizie. La retorica senza lumi dei* mass media *italiani* (Milano, Feltrinelli).

Luhmann, Niklas (2001): *La realtà dei* mass media (Milano, Franco Angeli).

Macchia, Alberto (2019): 'Spunti in tema di negazionismo', *Cassazione penale*, 1, pp. 22-31.

Manes, Vittorio (2017): 'La 'vittima' del 'processo mediatico': misure di carattere rimediale', *Diritto penale contemporaneo – Rivista trimestrale*, 3, pp. 114-128.

Manes, Vittorio (2019): 'Diritto penale *no-limits.* Garanzie e diritti fondamentali come presidio per la giurisdizione', *Questione giustizia*, 26 marzo 2019, disponibile a questo link.

Mantovani, Ferrando (2015): *Stupidi si nasce o si diventa? Compendio di stupidologia* (Pisa, ETS).

Mantovani, Giulia (2013): 'Se un comunicato-stampa può aiutare giudici e cittadini…', *Cassazione penale*, 11, pp. 3787-3798.

Mantovani, Giulia (2016): 'Informazione, presunzione d'innocenza a 'verginità del giudice'. L'Italia e l'Europa', in UCPI (eds.): *L'informazione giudiziaria in Italia. Libro bianco sui rapporti tra mezzi di comunicazione e processo penale* (Pisa, Pacini), pp. 128-136.

Marafioti, Luca (2010): 'Processi penali *by media*: un circolo vizioso?', in Resta (eds.): *Giustizia e* mass media*: quali regole per quali soggetti* (Napoli, Editoriale Scientifica), pp. 111-120.

Marandola, Antonella (2017): 'La tutela dell'identità personale (informatica), anche del soggetto coinvolto in un processo penale', *Processo penale e giustizia*, 3, pp. 371-379.

Martinelli, Silvia (2017): *Diritto all'oblio e motori di ricerca. Memoria e* privacy *nell'era digitale* (Milano, Giuffrè).

Mazzanti, Edoardo (2018): 'Processo mediatico e diritto all'oblio. Il possibile gioco di sponda tra UE e CEDU', in Mantelero e Poletti (eds.): *Regolare le tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna* (Pisa, Pisa University Press), pp. 379-393.

Meijer, Sonja (2017): 'Rehabilitation as a Positive Obligation', *European Journal of Crime, Criminal Law and Criminal Justice*, 25, pp. 145-162.

Miniussi, Davide (2015): 'Il 'diritto all'oblio": i paradossi del caso 'Google', *Rivista italiana di diritto pubblico comunitario*, 1, pp. 209-234.

Monti, Matteo (2018): 'La XVII Legislatura e la libertà d'espressione: un bilancio fra luci e ombre', *Osservatorio sulle fonti*, 2018, 2, pp. 1-22.

Murphy, Thérèse e Ó Cuinn, Gearóid (2010): 'Work in Progress: New Technologies and the European Court of Human Rights', *Human Rights Law Review,* 10, pp. 601-638.

Padovani, Tullio (2001): 'Poteri discrezionali e processo penale. Note e riflessioni su un fenomeno cangiante', in De Francesco e Campanella (eds.): *Scritti in onore di Antonio Cristiani* (Torino, Giappichelli), pp. 583-587.

Padovani, Tullio (2008): 'Informazione e giustizia penale: dolenti note', *Diritto penale e processo*, 6, pp. 689-692.

Palazzo, Francesco (2009): 'Mezzi di comunicazione e giustizia penale', *Politica del diritto*, 2, pp. 193-216.

Palazzo, Francesco (2012): 'Il giudice penale tra esigenze di tutela sociale e dinamica dei poteri pubblici', *Cassazione penale*, 5, pp. 1610-1627.

Palazzo, Francesco (2017): 'Note sintetiche sul rapporto tra giustizia penale e informazione giudiziaria', *Diritto penale contemporaneo – Rivista trimestrale*, 3, pp. 139-149.

Palazzo, Francesco (2018): 'Paura del crimine, rappresentazione mediatica della criminalità e politica penale (a proposito di un recente volume)', *Rivista di diritto dei media*, 3, pp. 14-21.

Palazzo, Francesco (2019): 'Il volto del sistema penale e le riforme in atto', *Diritto penale e processo*, 1, pp. 5-11.

Paliero, Carlo Enrico (1990): 'Il principio di effettività del diritto penale', *Rivista italiana di diritto e procedura penale*, 2, pp. 430-544.

Paliero, Carlo Enrico (2006): 'La maschera e il volto (percezione sociale del crimine ed 'effetti penali' dei *media*), *Rivista italiana di diritto e procedura penale*, 2, pp. 467-538.

Paliero, Carlo Enrico (2012): 'L'agorà e il palazzo. Quale legittimazione per il diritto penale?', *Criminalia*, pp. 95-117.

Paliero, Carlo Enrico (2014): 'Il diritto liquido. Pensieri post-delmasiani sulla dialettica delle fonti penali', *Rivista italiana di diritto e procedura penale*, 3, pp. 1099-1132.

Pardolesi, Roberto (2017): 'L'ombra del tempo e (il diritto al)l'oblio', *Questione giustizia*, 1, pp. 76-85.

Paulesu, Pier Paolo (1995): 'Presunzione di non colpevolezza', in *Digesto delle discipline penalistiche*, IX agg. (Torino, Utet), pp. 670-694.

Pecchioni, Gherardo (2019): 'Note sulle recenti modifiche alla disciplina della prescrizione', *disCrimen*, pp. 1-5.

Peron, Sabrina (2018): 'Il risarcimento danni da diffamazione tramite *mass-media*: analisi e riflessioni sui criteri orientativi proposti dall'Osservatorio sulla Giustizia Civile di Milano', disponibile a questo link.

Pezzella, Vincenzo (2016): *La diffamazione* (Milano, Wolters Kluwer).

Piergallini, Carlo (2012): "Civile' e 'penale' a perenne confronto: l'appuntamento di inizio millennio', in Roppo e Sirena (eds): *Il diritto civile, e gli altri* (Milano, Giuffrè), pp. 111-154.

Piergallini, Carlo (2014): 'Il fondamento della prescrizione nel diritto penale (ancora una volta) all'esame della Consulta', *Giurisprudenza costituzionale*, 3, pp. 2371-2381.

Piergallini, Carlo (2015): 'Autonormazione e controllo penale', *Diritto penale e processo*, 3, pp. 261-266.

Pietropaoli, Stefano (2017): 'La rete non dimentica. Una riflessione sul diritto all'oblio', *Ars interpretandi*, 1, pp. 67-80.

Pisapia, Alice (2017): 'Per una quantificazione economica della lesione del diritto all'oblio', *Questione giustizia*, 1, pp. 86-92.

Pitch, Tamar (2019): 'Il protagonismo della vittima', *disCrimen*, pp. 1-6.

Pitruzzella, Giovanni (2018): 'La libertà di informazione nell'era di Internet', *Rivista di diritto dei media*, 1, pp. 19-47.

Pollicino, Oreste (2014): 'Google rischia di 'vestire' un ruolo para-costituzionale', *Il Sole 24 Ore*, disponibile a questo link.

Pollicino, Oreste (2018): 'La prospettiva costituzionale sulla libertà di espressione nell'era di internet', *Rivista di diritto dei media*, 1, pp. 48-82.

Pollicino, Oreste (2019): 'Limitare il diritto all'oblio è un rischio', *Il Sole 24 Ore*, disponibile a questo link.

Pozzi, Walter G. (2011-2012): 'Il giornalismo degli orrori', *PaginaUno*, 25, pp. 22-29.

Pratt, John e Miao, Michelle (2017): 'Penal Populism: the End of Reason', disponibile a questo link.

Pugiotto, Andrea (2009): 'Quando (e perché) la memoria si fa legge', *Quaderni costituzionali*, 1, pp. 7-35.

Pugiotto, Andrea (2019): 'L'odierno protagonismo della vittima. In dialogo con Tamar Pitch', *disCrimen*, pp. 1-7.

Pulitanò, Domenico (2013): 'Populismi e penale. Sulla attuale situazione spirituale della giustizia penale', *Criminalia*, pp. 123-146.

Pulitanò, Domenico (2017): 'Selezione punitiva fra diritto e processo', in De Francesco e Gargani (eds.): *Evoluzione e involuzioni delle categorie penalistiche*, (Milano, Giuffrè), pp. 227-247.

Resta, Giorgio (2007): 'Identità personale e identità digitale', *Diritto dell'informatica*, 3, pp. 511-531.

Resta, Giorgio (2010): 'Il problema dei processi mediatici nella prospettiva del diritto comparato', in Id. (eds.): *Giustizia e* mass media*: quali regole per quali soggetti* (Napoli, Editoriale Scientifica), pp. 3-52.

Resta, Giorgio (2014): 'La morte digitale', *Diritto dell'informazione e dell'informatica*, 6, pp. 891-920.

Resta, Giorgio e Zeno-Zencovich, Vincenzo (2012): 'La storia 'giuridificata", in Resta e Zeno-Zencovich (eds.): *Riparare risarcire ricordare. Un dialogo tra storici e giuristi* (Napoli, Editoriale Scientifica), pp. 11-42.

Ricci, Annarita (2017): 'Sulla 'funzione sociale' del diritto alla protezione dei dati personali', *Contratto e impresa*, 2, pp. 586-612.

Riviezzo, Antonio (2018): 'L'ingiusto processo mediatico', *Rivista di diritto dei media*, 3, pp. 62-76.

Rodotà, Stefano (2006): *La vita e le regole* (Milano, Feltrinelli).

Rodotà, Stefano (2012a): *Il diritto di avere diritti* (Roma-Bari, Laterza).

Rodotà, Stefano (2012b): 'Il diritto alla verità', in Resta e Zeno-Zencovich (eds.): *Riparare risarcire ricordare. Un dialogo tra storici e giuristi* (Napoli, Editoriale Scientifica), pp. 497-516.

Rugani, Gabriele (2018): 'Il diritto all'oblio dell'articolo 17 Regolamento (UE) 679/2016: una grande novità? Una denominazione opportuna?', in Mantelero e Poletti (eds.): *Regolare le tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna* (Pisa, Pisa University Press), pp. 455-466.

Scaffardi, Lucia (2017): '*Data retention* e diritti della persona', in costituzionalismo.it, 2, pp. 55-87.

Signorato, Silvia (2018): 'Novità in tema di *data retention*. La riformulazione dell'art. 132 Codice *Privacy* da parte del d.lgs. 10 agosto 2018, n. 101', *Diritto penale contemporaneo*, 11, pp. 153-161.

Spangher, Giorgio (2016): 'Verità, verità processuale, verità mediatica, verità politica', *Diritto penale e processo*, 6, pp. 806-808.

Sparrow, Betsy, Liu, Jenny, Wegner, Daniel M. (2011): 'Google Effects on Memory: Cognitive Consequences of Having Information at Our Fingertips', *Science*, 333, pp. 776-778.

Stradella, Elettra (2017): 'Brevi note su memoria e oblio in rete a partire dal regolamento UE 679/2017', in Passaglia e Poletti (eds.): *Nodi virtuali, legami informali: Internet alla ricerca di regole* (Pisa, Pisa University Press), pp. 87-100.

Thiene, Arianna (2017): 'Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo', *Nuove leggi civili commentate*, 2, pp. 410-444.

Tripodi, Andrea Francesco (2019): 'Dal *diritto penale della paura* alla *paura del diritto penale*. Spunti per una riflessione', *Quaderno di storia del penale e della giustizia*, pp. 263-273.

Tucci, Giuseppe (2010): 'Processi mediatici, diritti inviolabili e tutela di diritto privato', in Resta (eds.): *Giustizia e* mass media*: quali regole per quali soggetti* (Napoli, Editoriale Scientifica), pp. 121-161.

Turchetti, Sara (2017): 'Diffamazione e trattamento dei dati personali nel processo mediatico', *Diritto penale contemporaneo – Rivista trimestrale*, 3, pp. 97-104.

Unione Camere Penali Italiane (2016), *L'informazione giudiziaria in Italia. Libro bianco sui rapporti tra mezzi di comunicazione e processo penale* (Pisa, Pacini).

Valentini, Cristiana (2016): 'La presunzione d'innocenza nella Direttiva n. 2016/343/UE: *per aspera ad astra*', *Processo penale e giustizia*, 6, pp. 193-204.

Vesto, Aurora (2018): 'La tutela dell'oblio tra intimità e condivisione senza filtri', *Rivista di diritto dei media*, 2, pp. 105-118.

Visconti, Arianna (2011): 'Teorie della pena e '*shame sanctions*': una nuova prospettiva di prevenzione o un caso di atavismo del diritto penale?', in Bertolino, Eusebi, Forti (eds.): *Studi in onore di Mario Romano* (Napoli, Jovene), pp. 633-675.

Visconti, Arianna (2017): 'Memoria e comprensione dell''altro' tra difesa sociale e garanzie individuali: la prospettiva giusletteraria per un diritto penale democratico', *Jus*, 1, pp. 35-82.

Voena, Giovanni Paolo (2017): 'Processo penale e mezzi di comunicazione di massa: un instabile stato dell'arte', *Processo penale e giustizia*, 6, pp. 1113-1132.

Zanini, Silvia (2018): 'Il diritto all'oblio nel Regolamento europeo 679/2016: *quid novi*?', federalismi.it, 15, pp. 1-21.

Zeno-Zencovich, Vincenzo (2007): 'Comunicazione, reputazione, sanzione', *Diritto dell'informatica*, 2, pp. 263-275.

La moltiplicazione dei garanti nel settore della tutela dei dati personali: riflessi penalistici del GDPR

La multiplicación de las garantías en el sector de la tutela de los datos personales: Reflexiones penalísticas del GDPR

The Multiplication of Responsibilities in the Personal Data Protection Area: Criminal Law Implications of the GDPR

Gaia Fiorinelli
Allieva perfezionanda in Diritto Penale presso la Scuola Superiore Sant'Anna di Pisa
gaia.fiorinelli@santannapisa.it

Abstracts

L'individuazione delle posizioni di garanzia nel settore della tutela dei dati personali costituisce un tema quasi inesplorato, sia da parte degli studiosi della materia, sia da parte della giurisprudenza, di merito e di legittimità. Tale tema, tuttavia, merita un rinnovato interesse a seguito dell'entrata in vigore del Regolamento Europeo per la Protezione dei Dati Personali e del relativo decreto di adeguamento (d.lgs.101/2018): è la stessa architettura di tali complessi normativi, infatti, a polarizzare l'attenzione sulla gestione del rischio e sulla *accountability* dei soggetti individuati quali garanti dell'integrità e della sicurezza dei dati e dei sistemi informatici. Il presente contributo mira, dunque, alla ricostruzione delle posizioni di garanzia nel settore della tutela dei dati e al conseguente inquadramento delle relazioni intersoggettive tra i garanti.

La individualización de las posiciones de garantía en el sector de la tutela de los datos personales constituye un tema casi inexplorado, tanto por la doctrina como por la jurisprudencia. No obstante, la entrada en vigencia del Reglamento Europeo de Protección de Datos Personales y del correspondiente decreto de adecuación (Decreto Legislativo 101/2018) justifican una mayor atención a esta materia. El presente artículo tiene por objeto analizar la reconstrucción de las posiciones de garantía en el sector de la tutela de los datos y el consecuente encuadramiento de las relaciones intersubjetivas entre las garantías.

The attribution of responsibility as a 'guarantor' in the area of personal data protection is a relatively unknown issue, both for the scholars and the case-law. The said topic, however, deserves to be (re-)investigated after the entry into force of the EU Regulation on Personal Data Protection, as implemented in Italy by the Legislative Decree no. 101/2018. The legal architecture itself focuses on risk management and accountability of those labelled as 'guarantors' of data integrity and security of networks. This paper aims to reconstruct the notion of 'guarantor' in the area of data protection as well as assessing the relationships among 'guarantors'.

Sommario

1. Il GDPR: impostazione preventiva e scopi di tutela.

Per quanto il *Regolamento Generale sulla Protezione dei Dati*[1] nulla disponga direttamente in materia penale[2], l'impostazione complessiva e gli scopi di tutela del *Regolamento* offrono, tuttavia, spunti di notevole interesse anche in una prospettiva penalistica.

Anzitutto, infatti, con l'entrata in vigore del *Regolamento* 679/2016 si è ulteriormente consolidato un approccio di stampo preventivo alla protezione dei dati personali[3]: il titolare del trattamento – sul quale ricade "la responsabilità generale per qualsiasi trattamento di dati personali" (*Considerando* n. 74) – è, infatti, tenuto ad adottare misure idonee a soddisfare i principi della "protezione dei dati fin dalla progettazione" e della "protezione dei dati per impostazione predefinita" (*Considerando* n. 78), così predisponendo già *prima* del trattamento adeguate forme di tutela *mediante la tecnologia*[4]; inoltre, al titolare è altresì richiesto di adottare misure di carattere tecnico e organizzativo adeguate per garantire, *durante* il trattamento, il rispetto delle disposizioni del *GDPR* (*Considerando* n. 78), per la tutela dei diritti e delle libertà delle persone fisiche[5].

Ulteriore riconferma di tale impostazione preventiva si ritrova, inoltre, nel *Considerando* n. 84, ove si prevede che il titolare del trattamento sia chiamato a svolgere una "valutazione d'impatto sulla protezione dei dati", qualora il trattamento stesso possa presentare un rischio elevato; mediante tale valutazione si dovrebbero determinare, in particolare, l'origine, la natura, la particolarità e la gravità del rischio, in modo da adottare misure specifiche ed opportune, per assicurare il rispetto del *Regolamento*.

Indicativo dell'importanza della struttura organizzativa è, altresì, l'art. 32 co. 4 del *Regolamento*, in forza del quale il titolare del trattamento è reso responsabile dei trattamenti effettuati da parte dei dipendenti inseriti nell'organigramma aziendale: si prevede, infatti, che il titolare debba far sì che «chiunque agisca sotto la [sua] autorità e abbia accesso ai dati personali» non possa, comunque, trattare tali dati se non sia stato destinatario di specifiche istruzioni in tal senso da parte del titolare.

Orbene, il generale principio di *accountability*[6], l'accento posto sulle misure *tecniche* ed *organizzative*, unitamente alla previsione di strumenti di *risk-assessment* – al fine di *prevenire* il *rischio* di violazioni – consentono di annoverare anche il *GDPR* tra quegli interventi normativi che portano a un progressivo consolidamento del paradigma di «prevenzione mediante organizzazione», con ciò intendendosi la correlazione che si viene a creare tra "gestione del rischio" e organizzazione dei fattori produttivi[7] o, in altri termini, la «estensione totalizzante dell'autoresponsabilità in ogni fase della vita dell'impresa»[8].

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

[2] Di diretto interesse penalistico è, infatti, soltanto il *Considerando* 149, ove si riconosce agli Stati membri la facoltà di prevedere sanzioni penali per le violazioni del *Regolamento* o delle norme nazionali adottate in attuazione del *Regolamento* stesso. Si prevede, inoltre, che tra le misure penali potrebbe altresì ricomprendersi la sottrazione dei profitti che siano stati illecitamente ottenuti, mediante violazioni di disposizioni del *Regolamento*. Da ultimo, si prescrive che l'adozione di sanzioni penali non possa, tuttavia, porsi in contrasto con il principio del *ne bis in idem*, per come interpretato dalla Corte di Giustizia dell'Unione Europea, rispetto alle sanzioni amministrative, già previste dal *Regolamento*. Sul d. lgs. 101/2018, adottato per adeguare la legislazione nazionale alle disposizioni del GDPR, v. Manes, Mazzacuva (2019), pp. 171 ss.; D'Agostino (2019); Labianca (2019), pp. 1004 ss.; Resta (2019), pp. 1019 ss.; Provolo (2019), pp. 242 ss.

[3] Cfr. D'Agostino (2019), p. 53: invero, il sistema di protezione dei dati personali delineato dal *GDPR* sembra «ruotare attorno al concetto di rischio».

[4] Cfr. Voigt e Von dem Bussche (2017), p. 38. È l'art. 25 del *Regolamento*, poi, a precisare che tali misure, finalizzate a "integrare nel trattamento le necessarie garanzie" possano consistere, ad esempio, nella pseudonimizzazione, nella minimizzazione, nonché in impostazioni predefinite tali da assicurare che siano trattati soltanto i dati personali necessari per ogni specifica finalità del trattamento.

[5] Cfr. Voigt e Von dem Bussche (2017), p. 38.

[6] Cfr. D'Agostino (2019), p. 17, che sottolinea come il principio dell'*accountability*, o dell'autoresponsabilizzazione, attribuisca peculiare importanza alla autodisciplina e alla *compliance*, facendo ricadere sul titolare e sul responsabile l'obbligo di individuare le misure necessarie per assicurare il rispetto di tutte le rilevanti disposizioni di legge.

[7] Così Gargani (2017), p. 509.

[8] Cfr. D'Agostino (2019), p. 17 e p. 52, ove l'Autore rileva come proprio le imprese, gli enti collettivi (o finanche i grandi attori economici) siano i soggetti sui quali la disciplina del Regolamento sembra essere stata plasmata, considerando l'importanza che assumono, nell'impostazione

Si tratta, del resto, di un paradigma di tutela che era stato già messo in luce non soltanto da parte della Corte di Cassazione Civile, a Sezioni Unite, che aveva riconosciuto come dal trattamento di dati personali derivino «obblighi organizzativi, gestionali e di sicurezza la cui corretta individuazione, oltre che dalle specifiche indicazioni normative, discende dalla considerazione della *funzione (di garanzia) della disciplina nel suo complesso*»[9], ma anche da parte della Corte di Cassazione Penale, che aveva ricostruito la posizione del titolare del trattamento, ponendo in luce l'esistenza, in capo a quest'ultimo, di «un potere decisionale in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati», che si estrinseca anche mediante la designazione dei soggetti responsabili e la gestione dei rischi specifici connessi al trattamento[10].

Inoltre, come si è anticipato, anche l'ampiezza degli orizzonti di tutela del *Regolamento* si rivela di estremo interesse. Infatti, oltre a tale rilevantissima evoluzione strutturale, il *Regolamento Generale sulla Protezione dei Dati* sembra ampliare le prospettive di tutela, dal momento che, come sottolineato dal *Considerando* n. 75, mediante le misure di *protezione* dei dati personali si intende far fronte ai rischi suscettibili di cagionare, addirittura, "un danno fisico, materiale o immateriale", ai diritti e alle libertà delle persone fisiche coinvolte[11].

È il *Considerando* n. 85, inoltre, a precisare che le "violazioni" dei dati personali possano rilevare anche in quanto suscettibili di tradursi direttamente in più gravi condotte lesive, tra cui discriminazione, furto, usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica[12].

Con il *GDPR* si è, infatti, portata a compimento la progressiva transizione da una tutela della riservatezza intesa in senso minimalistico quale diritto alla *non divulgazione* delle informazioni di carattere personale, a una tutela effettiva, intesa in un'accezione funzionale, che si traduce nel diritto alla *protezione* e al *corretto trattamento* dei dati personali, o in altre parole, nel diritto alla *corretta gestione* delle informazioni[13].

Ne deriva, dunque, un quadro composito, nel quale i soggetti individuati dal *Regolamento* quali garanti della protezione e della sicurezza dei dati – e nei cui confronti ricade, dunque, una responsabilità generale – vengono ad essere responsabilizzati in una pluralità di direzioni, a fronte, per l'appunto, della crescente natura plurioffensiva degli illeciti in materia di dati personali[14].

Non sembra azzardato, dunque, ipotizzare che possano configurarsi forme di responsabilità penale, a carico dei garanti della tutela dei dati, ulteriori rispetto alle sole fattispecie contenute nel *Codice privacy*: come si è detto, infatti, le violazioni delle disposizioni del *Regolamento* potrebbero chiamare in causa fattispecie ulteriori, connesse alla tutela dell'identità digitale, alla sicurezza dei sistemi informatici e finanche alla protezione della reputazione e del patrimonio[15]. Ad esempio, le c.d. *data breaches*, prese in considerazione dal *Regolamento* con riguardo agli obblighi di segnalazione e definite dall'art. 4 n. 12 come quelle violazioni di sicurezza che comportano «accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati», potrebbero con tutta evidenza acquisire rilevanza penale, ai sensi degli

generale del *GDPR*, gli obblighi di natura gestionale e organizzativa.

[9] Cfr. Ricci (2018), p. 2648, ove si richiama Cassazione civile., sez. un., 27 dicembre 2017, n. 30984, su *dejure.it*, ove, per l'appunto, espressamente si riconosce che «il legislatore richiede "modalità organizzative" ovvero *condotte positivamente rivolte* a tutelare la riservatezza dei dati».

[10] Cfr. Cassazione penale, sez. III, 17 dicembre 2013, n. 5107, su *dejure.it*; v. anche Manna, Di Florio (2019), pp. 902 ss.

[11] Cfr. Manna, Di Florio (2019), p. 936, ove si rileva, per l'appunto, come una delle novità più importanti del Regolamento consista proprio nella «qualificazione del diritto alla protezione dei dati personali come un diritto fondamentale delle persone fisiche (art. 1, par. 2)».

[12] Cfr. Manes, Mazzacuva (2019), p. 72, ove si sottolinea, per l'appunto, come la fattispecie di cui all'art. 167 del Codice privacy («Trattamento illecito di dati personali») risulti incentrata prevalentemente sulla tutela di beni giuridici individuali; in tal senso, la centralità del "nocumento" di cui alla medesima disposizione è chiaro indice della «logica di tutela personalistica» che si è perseguita con la riforma.

[13] In questi termini, cfr. in particolare D'Agostino (2019), p. 8 e p. 10: «il comune cittadino che fruisce dei servizi della società dell'informazione è posto nell'impossibilità di non svelarsi nell'agire quotidiano. Egli rilascia continuamente dati personali che scompongono la sua identità sociale in un catalogo di informazioni, perdendo lentamente il controllo di sé. Per questo la privacy, comunemente intesa nell'accezione minimale di *right to be let alone*, deve – come si è detto – «mutare il suo contenuto da diritto alla riservatezza a diritto all'autodeterminazione informativa»». In tal senso cfr. anche Torre (2004), p. 41.

[14] Come rilevato da Manes, Mazzacuva (2019), pp. 172 ss., infatti, l'attuale struttura della risposta (anche penale) agli illeciti in tema di dati personali affianca alla tutela di beni giuridici individuali anche una prospettiva di stampo più pubblicistico, che, sulla base di recenti casi di «utilizzo illecito di ingenti masse di dati personali» ha inteso fronteggiare anche «le ipotesi caratterizzate da maggiore diffusività lesiva».

[15] A tal proposito, per un catalogo delle fattispecie contenute nella parte speciale del codice penale che possano ricondursi all'ambito della tutela dei dati, cfr. Nauwelaerts (2018), pp. 84 ss.

artt. 615-*ter* c.p., 635-*bis* c.p. o 640-*ter* c.p.[16].

Anche in considerazione di tale progressivo ampliamento degli orizzonti di tutela pare opportuno, dunque, riflettere sulle implicazioni che tale «passaggio da una impostazione negativa e reattiva ad una positiva e proattiva della protezione dei dati personali»[17] può avere per il diritto penale.

2. La moltiplicazione dei garanti nel settore della protezione dei dati.

A fronte di tale generale responsabilizzazione del titolare del trattamento – che si traduce, come si è visto, nell'obbligo di adottare una pluralità di misure «il cui comune denominatore è la protezione preventiva del dato»[18] – il *Regolamento* si segnala, altresì, per una moltiplicazione dei garanti nel settore della tutela dei dati personali[19].

Invero, il GDPR prevede sin dalle *Definizioni* (art. 4) il coinvolgimento di una pluralità di soggetti nell'adempimento degli obblighi in esso previsti: accanto al «*titolare* del trattamento» (n. 7), ovverosia «la persona […] che determina le finalità e i mezzi del trattamento di dati personali», è prevista la figura del «*responsabile* del trattamento» (n. 8), vale a dire «la persona […] che tratta dati personali per conto del titolare del trattamento».

Infine, si aggiunge a queste figure anche il *responsabile della protezione dei dati personali* (o *DPO*), designato «in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati» e, quindi, della capacità di assolvere gli specifici compiti che, ai sensi del *GDPR*, gli devono essere affidati.

Il *Regolamento*, dunque, individua una serie di soggetti quali destinatari *iure proprio* di diversi compiti e ne istituzionalizza la cooperazione per l'assolvimento degli obblighi ivi previsti, mettendo allo stesso tempo in luce, al *Considerando* n. 79, la necessità di pervenire a *una chiara ripartizione delle responsabilità* tra i medesimi.

Ebbene, tale dettagliata articolazione dei ruoli e delle sfere di competenza dei soggetti coinvolti nel trattamento dei dati è di notevole interesse in una prospettiva penalistica. In particolare, l'indagine non può che essere svolta in primo luogo precisando e ricostruendo gli obblighi e i poteri impeditivi che ricadono su tali soggetti, e ciò tenendo conto che, nelle diverse proiezioni del "diritto penale del rischio", «l'analisi dei ruoli e delle responsabilità viene tematizzata entro la categoria giuridica della posizione di garanzia»[20]: strumento concettuale al quale è allora necessario far riferimento nell'analizzare le norme del *GDPR*. Come si è detto, infatti, a conferma dell'opportunità della prospettiva così tratteggiata, la latitudine degli obblighi previsti in capo a *titolare*, *responsabile* e *DPO*, comporta la necessità di verificarne le rispettive responsabilità penali non soltanto rispetto agli illeciti di cui agli artt. 167 e ss. del Codice Privacy, in forma commissiva, ma anche, in forma omissiva, rispetto a violazioni o persino a reati informatici commessi da parte di dipendenti o soggetti terzi[21].

Muovendo allora dal titolare del trattamento, egli è essenzialmente il soggetto obbligato ad adottare, in forza degli artt. 24 e 32 del *Regolamento*, adeguate misure tecniche ed organizzative, finalizzate a ridurre i rischi per la sicurezza (dei dati e, dunque) delle persone coinvolte[22]. In tal senso, dunque, al medesimo è indubbiamente ascrivibile un obbligo di garanzia *iure proprio*, rispetto alla tutela e alla sicurezza dei dati; obbligo che gli deriva direttamente dall'essere – ai sensi delle definizioni di cui all'art. 4 – colui che *determina le finalità e i mezzi*

[16] Cfr. in tal senso anche Luberto (2019), p. 948.
[17] Cfr. Ricci (2018) p. 2648.
[18] Cfr. Ricci (2018), p. 2648.
[19] Sul tema (sia pur con riguardo al diverso ambito dell'articolazione delle responsabilità penali in relazione all'abrogato reato di cui all'art. 169 del Codice Privacy), cfr. anche Picotti (2013), p. 68.
[20] Cassazione penale, sez. un., 24 aprile 2014, n.38343, su *dejure.it*.
[21] A tale ultimo proposito, v. Manna (2010), pp. 779 ss., anche in relazione alla diversa questione della configurabilità della fattispecie di cui all'art. 167 *Cod. privacy* in forma omissiva.
[22] Cfr. l'art. 24 GDPR: *1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.* Cfr. anche l'art. 32 GDPR: *1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.*

del trattamento di dati personali. In quanto fulcro del potere decisionale, il titolare del trattamento è, dunque, garante *originario*, rispetto alla liceità del trattamento e alla sicurezza dei dati; inoltre, egli è destinatario in via diretta dell'obbligo di predisporre trattamenti conformi alla disciplina del *GDPR*, di adottare adeguate misure di sicurezza, nonché di effettuare la c.d. *Valutazione d'impatto sulla protezione dei dati* (di cui all'art. 35). D'altra parte, la giurisprudenza penale era giunta ad analoghe conclusioni già prima dell'entrata in vigore del *Regolamento*, avendo rilevato come la pregnanza dei poteri decisionali che ricadono in capo al *titolare* del trattamento – in ordine alle finalità e alle modalità del trattamento, nonché, più in generale, in ordine alle misure funzionali alla "gestione dei rischi" – consentisse di ritenerlo destinatario di specifici obblighi di tutela[23]. Del resto, il contenuto di tali obblighi comprende non soltanto la conformità del trattamento alle disposizioni del *Regolamento*, ma anche la "protezione dei dati", tenuto conto dei rischi per le persone fisiche coinvolte nel trattamento: proprio in tale obbligo di garanzia, così, configurato, si coglie, dunque, quello "speciale vincolo di tutela" tra il soggetto garante e il titolare del bene, incapace di proteggerlo autonomamente[24], che consente di ipotizzare l'effettiva sussistenza di un obbligo di carattere *impeditivo*, nella forma dell'obbligo "di controllo", dovendo il titolare del trattamento adottare misure idonee a proteggere (i dati di) un novero indeterminato di soggetti[25] da rischi specifici, connessi allo svolgimento dell'attività.

Così determinati la fonte e lo specifico contenuto dell'obbligo in parola, occorre, dunque, valutare la sussistenza, quanto meno in astratto, di idonei poteri di carattere impeditivo, necessari perché sia configurabile una complessiva posizione di garanzia in capo al titolare del trattamento; ebbene, come si è anticipato, già la Corte di Cassazione aveva attribuito specifico rilievo alla circostanza che il *titolare* sia proprio colui che – in via esclusiva – determina le finalità e le modalità del trattamento, disponendo, dunque, di un'indiscussa signoria sulla fonte di rischio. Tali considerazioni consentono, perciò, di ritenere che il titolare del trattamento rivesta la funzione di "garante", rispetto alla tutela di tutti i dati personali che siano stati affidati alla sua protezione.

Indubbiamente più complessa è, invece, la focalizzazione del ruolo e delle responsabilità del *responsabile del trattamento*, identificabile in colui che, per l'appunto, *tratta dati personali per conto del titolare del trattamento*.

A tal proposito, per individuare gli obblighi e i poteri del *responsabile*, occorre anzitutto richiamare l'art. 28 *GDPR*, ove si stabilisce che il titolare del trattamento debba ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del *Regolamento* e garantisca la tutela dei diritti dell'interessato, così coinvolgendo direttamente anche il *responsabile* negli obblighi di adempimento alla normativa. Inoltre, la lett. f) co. 3 dell'art. 28 precisa che il responsabile assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 e, infine, l'art. 32 estende al responsabile – al pari del titolare – l'obbligo di mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio.

Dal complesso di tali disposizioni sembra di potersi concludere che anche il responsabile del trattamento sia – nell'articolazione del *GDPR* – destinatario di una serie di obblighi *iure proprio*, sia pur ben più specifici rispetto a quelli previsti in capo al *titolare*. Sulla base di quanto detto, dunque, si può ritenere che, nei limiti dei propri obblighi e, soprattutto, dei propri (limitati) poteri, anche il *responsabile del trattamento* sia titolare di una funzione di garanzia, quanto alla liceità del trattamento e alla sicurezza dei dati. A tal proposito, è utile rammentare come nella giurisprudenza di legittimità il *responsabile* del trattamento sia stato configurato alla stregua di un "preposto", il quale, dunque, nel limitato ambito cui sia stato adibito, riveste una funzione analoga a quella del *titolare* del trattamento e deve, dunque, essere considerato, in virtù di tale rapporto di preposizione, destinatario diretto di specifici obblighi di tutela[26]. È bene

[23] Cfr. Cassazione penale, sez. III, 17 dicembre 2013, n. 5107, su *dejure.it*.
[24] Cfr. Cassazione penale, sez. IV, 29 marzo 2019, n. 17491, su *dejure.it*. Sul tema specifico cfr. anche D'Agostino (2019), pp. 9-10: nella società dell'informazione, «la generalità dei consociati [rinuncia] tacitamente alla propria riservatezza e [rilascia] le proprie informazioni personali per accedere ai servizi offerti»; «il comune cittadino che fruisce dei servizi della società dell'informazione è posto nell'impossibilità di non svelarsi nell'agire quotidiano. Egli rilascia continuamente dati personali che scompongono la sua identità sociale in un catalogo di informazioni, perdendo lentamente il controllo di sé». Dopo che l'interessato ha "perso" il controllo sui propri dati ricade, pertanto, sul *titolare* del trattamento l'obbligo di assicurarne la protezione e la corretta gestione.
[25] Cfr. Alessandri e Seminara (2018), p. 59.
[26] Cfr. Cassazione penale, sez. III, 17 dicembre 2013, n. 5107, su *dejure.it*.

precisare, tuttavia, che l'obbligo di garanzia sussistente in capo al soggetto designato *responsabile* del trattamento dovrà avere un ambito ben circoscritto, non potendosi estendere all'intera gestione aziendale, ma limitandosi, nel contesto del trattamento svolto per conto del titolare, agli obblighi che il *Regolamento* configura direttamente in capo al *responsabile*, alle istruzioni impartite da parte del titolare, nonché, soprattutto, agli effettivi poteri di intervento[27].

Ancora più complessa è, infine, la figura, introdotta *ex novo* con il *Regolamento*, del *responsabile della protezione dei dati*, o *data protection officer* (*DPO*), cui è dedicata l'intera Sezione IV del Capo IV (relativo ai *Soggetti*).

L'art. 37 prevede, infatti, che il titolare e il responsabile del trattamento in taluni casi debbano[28] – e, comunque, possano[29] – nominare, all'interno della compagine aziendale, un *responsabile della protezione dei dati personali*. Tale soggetto deve essere, per l'appunto, designato in funzione delle sue qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere gli specifici compiti, di cui si dirà, previsti dall'art. 39 del *Regolamento*; per espressa indicazione, il *DPO* potrà essere un *dipendente* del titolare del trattamento, ovvero potrà essere legato a quest'ultimo da un contratto di servizi. L'art. 38 attribuisce, poi, al *DPO* connotati peculiari, prevedendo che il *titolare* e il *responsabile* debbano fornirgli le risorse necessarie per assolvere ai propri compiti, nonché che debbano garantire che allo stesso non sia impartita alcuna istruzione; il *Regolamento* configura così, con riguardo al *DPO*, una posizione denotata da autonomia e indipendenza, nell'assolvimento della propria funzione.

Quanto agli obblighi e ai poteri del *DPO*, l'art. 39 del *Regolamento* vi fa rientrare sia funzioni di natura essenzialmente consultiva e informativa – tra le quali il compito di informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento (lett. a) e di fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati, oltre a sorvegliarne lo svolgimento (lett. c) – sia funzioni di portata ben più vasta, tra le quali spicca, in particolare, il compito di *sorvegliare l'osservanza* del *Regolamento*, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo (lett. b).

Orbene, com'è evidente, le funzioni che rientrano nel primo ambito potrebbero anche portare a escludere un diretto coinvolgimento del *DPO* nelle responsabilità che ricadono sul *titolare* del trattamento; come si è osservato, la figura del *DPO* sarebbe, con riguardo a questo profilo, per certi versi assimilabile a quella del *Responsabile del Servizio di Prevenzione e Protezione*, il quale, come inizialmente riconosciuto dalla giurisprudenza di legittimità, non sarebbe titolare di una autonoma posizione di garanzia[30], in virtù dello svolgimento di una funzione di solo supporto informativo. La questione è, tuttavia, ben più complessa, già con riguardo a questo primo profilo, ove si consideri che la Suprema Corte ha, sul punto, progressivamente mutato orientamento, arrivando a ritenere che anche un soggetto che, all'interno della struttura aziendale, svolga un ruolo non gestionale ma di consulenza, abbia purtuttavia l'obbligo giuridico di adempiere diligentemente l'incarico affidatogli e, dunque, di collaborare con i vertici dell'impresa individuando i rischi connessi all'attività e fornendo le opportune indicazioni tecniche per risolverli, con la conseguenza che, in relazione a tale suo compito, potrà essere

[27] A tal proposito può essere utile ricordare quanto previsto dall'art. 82 *GDPR*: *Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento*.

[28] Recita, infatti, l'art. 37 *GDPR*: 1. *Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10*.

[29] In virtù dell'art. 37 par. 4 *GDPR*.

[30] In tal senso, v. Cassazione penale, sez. IV, 23 novembre 2012, n. 49821, su *dejure.it*, ove si esclude che il responsabile del servizio di prevenzione e protezione (art. 32 e 33 d.lgs. n. 81 del 2008) sia, in quanto tale, titolare di una posizione di garanzia penalmente rilevante ex art. 40 co. 2 c.p.; ma v. anche Cassazione penale, sez. IV, 10 maggio 2017, n. 27516, su *dejure.it*, ove si è riconosciuta l'esistenza di una posizione di garanzia, sussistente in capo al responsabile del servizio di prevenzione e protezione, ma limitata alla diligente valutazione dei rischi, in modo completo e idoneo, in ciò compendiandosi i suoi obblighi e poteri impeditivi, rispetto all'evento da prevenire. V. anche Massaro (2013), p. 357 ss., e in part. 362.

chiamato a rispondere, quale garante, degli eventi che si verifichino per effetto della violazione dei suoi doveri[31].

Le maggiori difficoltà nel definire il ruolo rivestito dalla figura del *DPO* derivano, tuttavia, dalla citata lett. b) dell'art. 39, ove si annovera tra i compiti del *DPO* anche l'obbligo, di portata generale, di sorvegliare l'osservanza del *Regolamento* e delle altre disposizioni rilevanti in tema di protezione dei dati[32]. È necessario comprendere, infatti, se tale obbligo, ove letto in combinazione con i poteri riconosciuti al *DPO* dall'art. 38 del *Regolamento*, costituisca pur sempre obbligo di mera sorveglianza, o venga a configurarsi come obbligo di *garanzia*[33].

Affatto peculiari sono, infatti, le posizioni di coloro che siano destinatari di un generale obbligo, per così dire, di "vigilare sull'osservanza della legge", com'è il caso, ad esempio, dei membri del collegio sindacale ai sensi dell'art. 2403 c.c., oppure dei membri dell'Organismo di Vigilanza costituito ai sensi del d. lgs. 231/2001[34]; a tal proposito, infatti, nonostante le indicazioni di segno contrario provenienti dalla dottrina, la Corte di Cassazione ha a più riprese affermato che un dovere consistente nel "controllo di legalità", qual è quello che ricade, ad esempio, sui membri del collegio sindacale, comporti, ove violato, un coinvolgimento in eventuali reati commessi da parte dei soggetti vigilati, a titolo di omesso impedimento del reato altrui[35]. Né pare che la questione possa essere agevolmente risolta mediante uno scrutinio dei poteri di tipo fattuale e giuridico di cui dispone il *DPO*, che si risolvono essenzialmente in poteri cognitivi e di segnalazione. A tal proposito, infatti, nonostante si sia da più parti rilevata l'esigenza di escludere l'applicazione del meccanismo imputativo di cui all'art. 40 co. 2 c.p. in tutte le ipotesi in cui la legge imponga meri obblighi di sorveglianza[36], accompagnati da poteri di intervento c.d. "deboli"[37], è pur vero che, secondo l'impostazione giurisprudenziale dominante[38], un potere-dovere di segnalazione e di informazione – qual è quello che grava sul *DPO* – costituisce una sorta di potere di intervento "mediato", funzionale a sollecitare azioni impeditive altrui[39]. Si tratta, com'è evidente, di una questione di amplissimo respiro, che si inscrive nel tema della responsabilità dei soggetti controllori per l'omesso impedimento del reato da parte dei soggetti controllati[40].

Ciò che si vuole rilevare è, tuttavia, come tale disciplina renda estremamente complesso definire la posizione di garanzia riconducibile al *DPO*. Se, infatti, con riguardo a taluni aspetti potrebbe escludersi che lo stesso sia titolare di una autonoma posizione di garanzia, radicando tale conclusione nei connotati di *professionalità* e nelle funzioni di *consulenza* attribuite a tale soggetto[41], tuttavia l'autonomia e l'indipendenza che il *GDPR* attribuisce al *DPO*, nonché l'obbligo – *iure proprio* – di tenere conto dei rischi del trattamento[42] e, soprattutto, la previsione di un generale dovere di sorveglianza sull'applicazione del *Regolamento* da parte dei soggetti

[31] In questi termini, Cassazione penale, sez. un., 24 aprile 2014, n. 38343, su *dejure.it*.
[32] Sul punto cfr. Working Party Article 29 (2017), p. 17: nell'obbligo di sorvegliare la *compliance* rientrano i compiti relativi alla raccolta di informazioni, al fine di identificare i processi rilevanti e, dunque, di analizzarne la conformità con il *Regolamento*; inoltre, è richiesto al *DPO* di informare, consigliare e fornire proposte di miglioramento al *titolare* e al *responsabile* del trattamento.
[33] A tal proposito è necessario rinviare a Leoncini (1999), p. 7, che sottolinea la differenza sussistente tra obblighi di *garanzia*, la cui violazione può dar luogo a responsabilità *ex* art. 40 co. 2 c.p., e obblighi di *attivarsi* e di *sorveglianza*, la cui inosservanza non può mai dare luogo a responsabilità in forma omissiva. In tal senso, in quanto obbligo di controllare l'altrui operato, dovrebbe trattarsi in questo caso di un semplice obbligo di sorveglianza (capace di configurare, dunque, in capo al *DPO* un obbligo di segnalazione e informazione, ma non un obbligo di intervento). In senso analogo cfr. Working Party Article 29 (2017), p. 4 e p. 24: il *DPO* non è personalmente responsabile per la *non-compliance* con i requisiti di *data protection* posti dal *Regolamento*.
[34] Cfr. sul punto Bisori (1997); Giunta (2006); Centonze (2009); Consulich (2015).
[35] Cfr. da ultimo Cassazione penale, sez. V, 18 febbraio 2019, n. 12186, su *dejure.it*, nonché Centonze (2009), pp. 227 ss.
[36] Cfr. Ambrosetti, Mezzetti, Ronco (2012), p. 109.
[37] Cfr. Giunta (2006), p. 608.
[38] In giurisprudenza cfr. da ultimo Cassazione penale, sez. IV, 01 febbraio 2018, n. 9167, su *dejure.it*, nonché Cassazione penale, sez. IV, 12 gennaio 2016, n. 20050, su *dejure.it*, ove si statuisce l'equivalenza, ai fini della configurabilità di una posizione di garanzia, tra "poteri atti a impedire la lesione del bene garantito" e la disponibilità di "mezzi idonei a sollecitare gli interventi necessari a evitare che l'evento dannoso sia cagionato".
[39] Sulla configurazione di poteri impeditivi di carattere mediato, cfr. in generale Gargani (2017), p. 523; Consulich (2015), p. 444, ove si rileva come sia proprio «il concetto di *potere impeditivo mediato* che potrebbe consentire di predicare l'esistenza di una responsabilità omissiva per tutti coloro che sono parte necessaria, seppure non sufficiente, di una procedura impeditiva». Osserva Giunta (2006), p. 608, come, invece, possano ritenersi effettivamente impeditivi soltanto quei poteri cui corrispondano «doveri di conformazione, in quanto il loro esercizio produce effetti giuridici vincolanti sull'attività del soggetto controllato, e più in generale i poteri di blocco dell'attività del controllato». Anche De Francesco (2012), p. 3929, rileva come «l'allentamento della verifica dell'autonoma e concreta capacità impeditiva della condotta doverosa» sia evidente soprattutto laddove si configurino «meri 'obblighi di sorveglianza' rispetto all'altrui operato».
[40] Cfr. ancora Giunta (2006); Centonze (2009); Consulich (2015).
[41] Sulle *Garantenstellungen* di esperti e consulenti, v. Gargani (2017), p. 521; Basile (2018).
[42] Cfr. l'art. 39 par. 2, ove si prevede che *2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo*.

coinvolti contribuiscono a configurare una figura di carattere "ibrido", che non consente di risolvere in senso certamente negativo la questione circa la possibile sussistenza di una posizione di garanzia rilevante ai fini della presente indagine[43].

Ad ogni modo, pare che anche nelle maglie del *Regolamento* sia possibile cogliere quei due distinti paradigmi che si sono progressivamente affermati nel campo delle *Garantenstellungen* individuali[44]: da un lato, con riguardo alla posizione del *titolare* (e, volendo, del *responsabile*), si è, infatti, costituito un «modello di garanzia incentrato sulla sicurezza mediante prevenzione del rischio lecito»; dall'altro, con riferimento alla posizione del *DPO*, si è, invece, prefigurata una posizione per certi versi riconducibile al modello della «prevenzione del rischio illecito»[45], trattandosi di un soggetto tenuto non già alla tutela *diretta* dei beni coinvolti, quanto, come detto, alla più generale sorveglianza del rispetto di tutte le disposizioni rilevanti in materia.

3. Le relazioni intersoggettive tra i garanti della sicurezza: affidamento e trasferimento di funzioni di tutela.

L'analisi dei ruoli e delle responsabilità dei diversi soggetti normativamente previsti non può, certo, arrestarsi alla mera individuazione delle singole posizioni di garanzia: la sussistenza di vincoli di tutela che, in quanto reticolari, sono altresì interdipendenti, richiede, infatti, di confrontarsi con il tema delle relazioni intersoggettive tra i garanti[46] della tutela dei dati, al fine di comprendere, in particolare, la funzione e l'efficacia, rispetto al *titolare del trattamento*, della nomina del *responsabile del trattamento* e del *responsabile della protezione dei dati*.

A tal proposito, nel vigore della originaria disciplina in materia di protezione dei dati personali di cui alla l. 675 del 1996, si riteneva che il «potere-dovere», rimesso al titolare del trattamento, di decidere e, dunque, indirizzare i trattamenti, non fosse derogabile né, tantomeno, delegabile[47], cosicché non potessero nemmeno ipotizzarsi forme di trasferimento di funzioni dotate di efficacia liberatoria o quantomeno modificativa dell'originaria posizione di garanzia.

È necessario, tuttavia, verificare se tali conclusioni possano dirsi ancora attuali, dal momento che il *Regolamento* disciplina nel dettaglio le relazioni tra il *titolare* e i suoi "ausiliari", determinando non soltanto i requisiti che devono caratterizzare ciascun soggetto, ma anche le formalità relative agli atti di nomina, nonché l'efficacia di tali scelte organizzative sull'articolazione delle relative responsabilità.

Muovendo dalle relazioni tra il *titolare* e il *responsabile* del trattamento, quest'ultimo può, come si è anticipato, essere considerato una sorta di "preposto" il quale, in virtù delle norme del *Regolamento* e delle istruzioni impartite dal *titolare*, è destinatario *iure proprio* di obblighi di adeguamento e di impedimento, ma non è dotato di un'autonomia tale da poter in alcun modo esonerare da responsabilità il *titolare* del trattamento in caso di violazioni[48].

A riconferma di ciò è possibile richiamare la stessa nomenclatura utilizzata dal *GDPR*: se, infatti, la traduzione italiana crea ambiguità, è utile osservare come nel testo originale il *titolare* sia definito *controller*, mentre il *responsabile* sia, invece, un mero *processor*, cui può essere affidato, dunque, un complesso di funzioni di carattere meramente tecnico-esecutivo.

A fronte di ciò è, tuttavia, interessante osservare quanto previsto dall'art. 28 par. 10 del *Regolamento*, ove si prevede che laddove un responsabile del trattamento violi il *Regolamento*, determinando autonomamente le finalità e i mezzi del trattamento, egli sarà considerato un titolare del trattamento in questione. Proprio questa disposizione, infatti, può costituire, in un certo senso, un indice della impossibilità per il *titolare* del trattamento di delegare ad altri le principali funzioni decisionali che gli sono affidate dal *Regolamento*, essendo precluso al *responsabile* qualsiasi intervento nella determinazione generale delle *finalità* e dei *mezzi* del trattamento. Di tale disposizione può, al contempo, darsi una diversa lettura: tale norma, infat-

[43] Ritiene Calzolaio (2017), p. 620, che il vero ruolo che il DPO assume è quello di importare, nell'organizzazione del Titolare del trattamento, l'esperienza maturata ed aggiornata in merito alle migliori pratiche attuative ed alle politiche *della privacy by design e by default.*
[44] Cfr. Gargani (2017), p. 515: si tratta di due distinti paradigmi, accomunati dal medesimo referente teleologico-funzionale, rappresentato dal rischio.
[45] Cfr. ancora Gargani (2017), p. 515.
[46] Cfr. Gargani (2017), pp. 514-516 e De Francesco (2012), pp. 3927 ss.
[47] Cfr. Blaiotta (1999), p. 1643.
[48] Cfr. ancora Blaiotta (1999), p. 1643, che qualifica come meramente "operativi" i compiti affidati al responsabile del trattamento da parte del titolare.

ti, può essere considerata una sorta di clausola di equiparazione tra soggetti di fatto e soggetti di diritto, cosicché, nel caso in cui le competenze attribuite o le funzioni svolte dal soggetto che sia formalmente *responsabile* del trattamento arrivino fino alla determinazione *autonoma* delle finalità o dei mezzi del trattamento[49], lo stesso vedrà ricadere su di sé gli obblighi previsti in capo al precedente *titolare del trattamento*, potendosi così ipotizzare un trasferimento – o, meglio, un ampliamento[50] – della corrispondente posizione di garanzia.

Quanto, poi, al diverso tema delle relazioni intersoggettive tra titolare-responsabile del trattamento e *DPO*, è necessaria anche in questo caso qualche ulteriore precisazione.

Come si è anticipato, infatti, in forza dell'art. 38 del *Regolamento* il *DPO* si trova a rivestire una posizione connotata da autonomia e indipendenza nell'assolvimento dei propri compiti, che si traducono in una funzione informativo-consultiva e in una funzione di sorveglianza; inoltre, l'art. 37 – ove si specifica il requisito dell'idoneità professionale del *DPO* – e le prime indicazioni operative in materia[51] portano a ritenere che il *DPO*, in forza della "conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati" possa anche essere attivamente coinvolto nell'adempimento degli obblighi di *compliance*.

Tale molteplicità di funzioni richiede, dunque, di interrogarsi sulle relazioni funzionali che si vengono a creare tra il *DPO* e i garanti "originari", nella predisposizione delle misure tecniche e organizzative necessarie per la protezione dei dati, dovendosi verificare quali siano gli effetti – ai fini dell'articolazione delle responsabilità – dell'eventuale scelta di demandare al *DPO* decisioni di carattere tecnico od operativo.

Ebbene, a tal proposito, è possibile rammentare, in una prospettiva pratico-applicativa, la già richiamata giurisprudenza della Corte di Cassazione relativa alla figura del *Responsabile del Servizio di Protezione e Prevenzione*, ove si è confermato, a più riprese, che il ruolo dallo stesso svolto non possa essere in alcun modo assimilabile a quello di un "delegato", trattandosi di una figura normativamente individuata e, dunque, destinataria di *investitura* e non di *delega di funzioni*[52]. Considerazioni di egual segno potrebbero, allora, svolgersi anche con riferimento alla figura del *DPO*, soprattutto nelle ipotesi in cui la sua nomina sia prevista obbligatoriamente dal *GDPR*. È necessario osservare, tuttavia, come l'art. 39, nel prevedere che il *DPO* sia incaricato "almeno" dei compiti che vi sono elencati, non escluda la possibilità di un più ampio coinvolgimento dello stesso *DPO* nell'adempimento degli obblighi di *compliance*, proprio in virtù della richiamata conoscenza specialistica e della funzione di supporto che lo stesso è chiamato a svolgere rispetto al vertice dell'impresa. In tali ipotesi, infatti, ove si considerino l'autonomia decisionale (e finanche di spesa) di cui è dotato il *DPO*, si potrebbe allora ipotizzare che sul *titolare* del trattamento rimanga soltanto un più generale obbligo di *vigilanza*, trasferendosi sul *DPO* l'autonomia decisionale di carattere *tecnico*, rispetto all'individuazione delle *best practices* per l'adempimento degli obblighi previsti dal *GDPR*.

È, ad ogni modo, indubbio che il tema della relazione tra *titolare* e *DPO* si collochi nella ben più ampia questione della "scissione tra potere organizzativo-decisionale e sapere tecnico-scientifico"[53]; una questione che, purtuttavia, è essenzialmente ignorata nella prassi applicativa, com'è reso evidente dalla perdurante tendenza ad accentrare sul vertice dell'impresa (e sul destinatario diretto dei precetti penali) le rispettive responsabilità[54].

Anche dalla presente analisi emerge, infatti, tale tendenza all'accentramento dei poteri – e delle responsabilità – in capo al *titolare* del trattamento, atteso che, come si è visto, non sembra che atti di investitura o di delega possano con certezza limitarne la complessiva posizione di garanzia.

Ebbene, in tale scenario è allora interessante osservare come nel *Regolamento* sia stato introdotto, all'art. 26, l'istituto della *contitolarità*, quale strumento funzionale a dare evidenza

[49] Cfr. a tal proposito Gargani (2017), p. 518, ove si specifica la questione dei "garanti di fatto", con riguardo a tutte le ipotesi di «scissione tra titolarità formale della qualifica soggettiva e il reale e concreto esercizio della funzione corrispondente».
[50] Cfr. ancora Gargani (2017), pp. 518-519, ove si rileva come le clausole di equiparazione tra soggetti di diritto e soggetti di fatto e le norme estensive della qualifica comportino la «proliferazione di nuove e ulteriori posizioni di garanzia».
[51] Cfr. ad es. Working Party Article 29 (2017), p. 13.
[52] D'Alessandro (2016), p. 242, che sottolinea l'importanza di distinguere l'attribuzione in via originaria di ruoli funzionali tipizzati dalla legge, dalla delega di funzioni, che determina un decentramento derivato di poteri decisionali. V. anche Cassazione penale, sez. IV, 26 aprile 2017, n. 24958, su *dejure.it*, ove si afferma che la mera designazione del responsabile del servizio di prevenzione e protezione non costituisca una delega di funzioni e non sia dunque sufficiente a sollevare il datore di lavoro ed i dirigenti dalle rispettive responsabilità in tema di violazione degli obblighi dettati per la prevenzione degli infortuni sul lavoro.
[53] Cfr. Gargani (2017), p. 521.
[54] Sul tema delle incompetenze tecnico-scientifiche del vertice dell'impresa, cfr. Keller (2018), p. 113 ss.

alla segmentazione dei poteri decisionali. Con tale strumento si prevede, infatti, in modo espresso la possibilità, per i contitolari di un medesimo trattamento, di determinare mediante un accordo le aree di rispettiva competenza e, dunque, di rispettiva responsabilità: tale istituto si rivela, dunque, di particolare interesse, nella prospettiva che ci occupa, poiché attribuisce rilievo giuridico all'eventuale coinvolgimento di più soggetti nella determinazione delle finalità e dei mezzi del trattamento, e, dunque, risponde all'esigenza di saper distinguere tra le singole posizioni *funzionali* all'interno dell'organizzazione, «evitando irragionevoli "livellamenti" tra le incombenze dei soggetti» chiamati singolarmente a rivestirle[55].

4. Conclusioni.

Il sensibile mutamento di prospettiva adottato con il *Regolamento Generale sulla Protezione dei Dati* è, dunque, destinato indubbiamente a irradiare i suoi riflessi anche in materia penale: ciò, non soltanto in conseguenza dell'ampliamento dell'oggetto e delle funzioni della tutela, nell'era della *datification*[56], ma anche in virtù del dichiarato cambiamento di approccio, da una disciplina incentrata sui diritti dell'interessato – quale era l'originaria direttiva 95/46 – alla attuale «tutela preventiva fondata sulla strutturale e dinamica responsabilizzazione della filiera soggettiva coinvolta nel trattamento dei dati personali»[57].

Peraltro, come si è detto, anche in tale settore acquisisce una crescente importanza il fattore organizzativo, attesa la rilevanza cruciale assunta dall'adozione di modelli organizzativi funzionali alla prevenzione degli illeciti provenienti non già dall'esterno, ma anche dall'interno dell'organizzazione, mediante, per l'appunto, controlli e processi di formazione che assicurino il rispetto della normativa – e, dunque, la prevenzione del rischio-illecito – da parte dei dipendenti dell'impresa[58].

L'analisi della nuova disciplina in materia di protezione di dati personali è occasione, dunque, per formulare talune considerazioni di carattere più ampio, relative al tema, ben più vasto, dei rapporti tra diritto, responsabilità e tecnica, in connessione con la complessità delle organizzazioni.

Sembra, infatti, che a fronte della crescente importanza di una tutela (anche penale) dei dati personali e dell'integrità dei sistemi tecnologici nella società dell'informazione, anche il settore informatico-digitale possa aggiungersi a quei campi in cui la preponderanza della tecnica può portare a un problematico disallineamento tra poteri, doveri e responsabilità, disallineamento che, invece, proprio uno strumento quale la delega di funzioni potrebbe contribuire a risolvere, valorizzando competenze differenziate[59].

Invero, nella prospettiva dei rapporti tra tecnica e diritto, se l'affiancamento di prescrizioni giuridiche e prescrizioni tecniche nel tessuto del *Regolamento Generale sulla Protezione dei Dati* sembra non aver attribuito interamente «al detentore del potenziale pericoloso la potestà decisionale sulla misura del rischio consentito»[60] e sugli strumenti con il quale contrastarlo, tuttavia l'indissolubile integrazione tra dato tecnico e norma giuridica accresce la complessità dei rapporti tra i soggetti detentori del potere decisionale-organizzativo e le figure che, invece, apportano un sapere tecnico nelle procedure di gestione del rischio.

A prescindere dal dato normativo, dunque, è evidente che anche con riguardo alla tutela dei dati personali dovranno essere opportunamente valorizzati quegli atti organizzativi che determinino il coinvolgimento cooperativo di soggetti diversi nell'adempimento degli obblighi di tutela prescritti dal *Regolamento*[61], al fine di ripartire le responsabilità penali ricondu-

[55] In tal senso De Francesco (2012), p. 3929.
[56] Per questo concetto si rinvia a Calzolaio (2017), p. 598.
[57] Cfr. ancora Calzolaio (2017), p. 614.
[58] Come si è detto, riprendendo la classificazione di Gargani (2017), p. 515, si potrebbe, dunque, ritenere che con il *GDPR* si configurino sia forme di prevenzione del rischio *lecito*, sia forme di prevenzione del rischio *illecito*.
[59] Competenze che, nell'era della "tecnicizzazione", si trasformano in uno strumento di potere, per cui v. Calzolaio (2017), *passim*: «l'evoluzione tecnica (tecnicizzazione) aveva la forza di incrementare tutti i presupposti dell'universo dell'esperienza, con ciò modificando le dinamiche del potere come mezzo di comunicazione (e della struttura sociale)».
[60] A tal proposito, v. Stella (2003), p. 57.
[61] Cfr. Gargani (2017), p. 520. V. anche la soluzione adottata da Cassazione penale, sez. IV, 30 settembre 2015, n. 10177, su *dejure.it*, ove si è ritenuto che l'apporto fornito dal responsabile del servizio di prevenzione e protezione sia parte inscindibile di una procedura complessa che sfocia nelle scelte operative compiute dal titolare dell'impresa, cosicché la sua attività possa senz'altro rilevare ai fini della spiegazione causale dell'evento illecito, e anche la pronuncia di Cassazione penale, sez. IV, 23 novembre 2012, n. 49821, su *dejure.it*, secondo cui il responsabile

cendo ad unità tale moltiplicazione dei garanti.

Bibliografia

Alessandri (2010): *Diritto penale e attività economiche* (Bologna, Il Mulino).

Id. (2005): "Attività d'impresa e responsabilità penali", *Riv. it. dir. proc. pen.*, 2, pp. 534 ss.

Alessandri e Seminara (2018): *Diritto penale commerciale*, Vol. 1 (Torino, Giappichelli).

Ambrosetti, Mezzetti, Ronco (2012): *Diritto penale dell'impresa* (Bologna, Zanichelli).

Basile (2018): *Consiglio tecnico e responsabilità penale: il concorso del professionista tramite azioni 'neutrali'* (Milano, Giuffrè).

Bisori (1997): "L'omesso impedimento del reato altrui nella dottrina e nella giurisprudenza italiane", *Rivista italiana di diritto e procedura penale*, pp. 1340 ss.

Blaiotta (1999): "Le fattispecie penali introdotte dalla legge sulla privacy", *Cassazione penale*, 5, pp. 1642 ss.

Calzolaio (2017): "Protezione dei dati personali (dir. pubbl.)", *Digesto delle discipline pubblicistiche*, Agg., pp. 594 ss. (Torino, UTET).

Centonze (2009): *Controlli societari e responsabilità penale* (Milano, Giuffrè).

Consulich (2015): "Vigilantes puniri possunt. I destini dei componenti dell'organismo di vigilanza tra doveri impeditivi e cautele relazionali", *Rivista trimestrale di diritto penale dell'economia*, pp. 425 ss.

D'Agostino (2019): "La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101", *Archivio penale*, 1.

D'Alessandro (2016): "Delega di funzioni (diritto penale)", *Enciclopedia del diritto,* Annali, IX, pp. 241 ss. (Milano, Giuffrè).

De Francesco (2012): "Il concorso di persone e il dogma causale: rilievi critici e proposte alternative", *Cassazione penale*, 11, pp. 3913 ss.

Gargani (2017): "Posizioni di garanzia nelle organizzazioni complesse: problemi e prospettive", *Rivista trimestrale di diritto penale dell'economia*, 3-4, pp. 508 ss

Giunta (2006), "Controllo e controllori nello specchio del diritto penale societario", *Rivista trimestrale di diritto penale dell'economia*, pp. 597 ss

Keller (2018): "L'irrilevanza penale delle (in)competenze tecnico-scientifiche del datore di lavoro indispensabili per la valutazione dei rischi", *Diritto penale contemporaneo*, 10, pp. 113 ss.

Labianca (2019): "Il sistema delle tutele nel Regolamento Europeo n. 679/2016 sulla protezione dei dati personali", in Cadoppi, Canestrari, Manna, Papa, *Cybercrime*, (Milano, UTET), pp. 977 ss.

Leoncini (1999): *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza* (Torino, Giappichelli).

Luberto (2019): "*Data breach* e delitto dell'art. 168 D.Lgs. n. 196/2003", in Cadoppi, Canestrari, Manna, Papa, *Cybercrime*, (Milano, UTET), pp. 942 ss.

del servizio di prevenzione e protezione può diventare titolare di una posizione di garanzia penalmente rilevante se coinvolto direttamente nell'esercizio di poteri gestionali.

Manes, Mazzacuva (2019): "GDPR e nuove disposizioni penali del Codice privacy", *Diritto penale e processo*, 2, pp. 171 ss.

Manna, Di Florio (2019): "Riservatezza e diritto alla *privacy*", in Cadoppi, Canestrari, Manna, Papa, *Cybercrime*, (Milano, UTET), pp. 891 ss.

Massaro (2013): *La responsabilità colposa per omesso impedimento di un fatto illecito altrui* (Napoli, Jovene).

Nauwelaerts (2018): *Data Protection & Privacy* (Londra, Law Business Research).

Picotti (2013): "La tutela penale della persona e le nuove tecnologie dell'informazione", in Id., *Tutela penale della persona e nuove tecnologie*, (Padova, Cedam), pp. 29 ss.

Piergallini (2017): "Colpa (diritto penale)", *Enciclopedia del diritto,* Annali, X, pp. 222 ss.

Provolo (2019): "Il sistema sanzionatorio del novellato Codice della *privacy* e la tutela penale *patchwork* dei dati genetici e dei dati biometrici", *Rivista trimestrale di diritto penale dell'economia*, 2, pp. 242 ss.

Resta (2019): "I reati in materia di protezione dei dati personali", in Cadoppi, Canestrari, Manna, Papa, *Cybercrime*, (Milano, UTET), pp. 1019 ss.

Ricci (2018): "Trattamento di dati sensibili e principio di responsabilizzazione", *Giurisprudenza italiana*, 12, 2641 ss.

Stella (2003): "La costruzione giuridica della scienza: sicurezza e salute negli ambienti di lavoro", *Rivista italiana di diritto e procedura penale*, 1, 55 ss.

Torre (2004), "La gestione del rischio nella disciplina del trattamento dei dati personali", in Picotti, *Il diritto penale dell'informatica nell'epoca di internet*, (Padova, Cedam), pp. 237 ss.

Voigt e Von dem Bussche (2017): *The EU General Data Protection Regulation* (*GDPR)* (Cham, Springer).

Working Party Article 29 (2017): *Guidelines on Data Protection Officers ('DPOs')*, *ec.europa.eu*.

Corporate liability e compliance in the *cyber privacy crime*: il nuovo "modello organizzativo *privacy*"

Responsabilidad corporativa y compliance en el delito de privacidad cibernética:El nuevo "modelo organizativo de privacidad"

Corporate Liability and Compliance in the Cyber Privacy Crime: the New "Privacy Organizational Model"

Valentina Aragona
Dottoranda di ricerca presso l'Università Luiss Guido Carli di Roma
valentina.aragona@luiss.it

Riciclaggio | Lavado de activos | Money Laundering

Abstracts

L'esigenza di garantire un'adeguata protezione dai rischi in materia di trattamento illecito dei dati personali provenienti dallo spazio virtuale ha messo in luce lo stretto legame esistente tra *cybercrime* e *privacy* e ha condotto il legislatore europeo a valorizzare il momento della prevenzione, incentivando l'adozione di efficaci misure di protezione dei dati personali nelle reti e nei sistemi informatici. Il GDPR adotta un nuovo approccio basato sul rischio, ponendo in evidenza come il trattamento illecito dei dati personali non sia frutto della condotta del singolo, ma derivi da una precisa politica di impresa. Ciò induce a interrogarsi circa la possibilità di costruzione e adozione di un modello organizzativo integrato, che garantisca un coordinamento tra la disciplina di cui al D.Lgs. n. 231/2001 e la normativa in materia di *privacy*[*].

La exigencia de garantizar una adecuada protección de los riesgos en material de tratamiento ilícito de los datos personales provenientes del espacio virtual ha puesto en evidencia la estrecha relación entre cibercrimen y privacidad, provocando que el legislador europeo haya comenzado a preocuparse de la prevención de tales conductas, incentivándola adopción de medidas de protección eficaces de los datos personales en la red y en los sistemas informáticos. El GDPR adopta un nuevo enfoque basado en el riesgo, destacando cómo el tratamiento ilícito de datos personales no es fruto de la conducta del individuo, sino que deriva de una precisa política de empresa. Ello lleva a interrogarse acerca de la posibilidad de construir y adoptar un modelo de organización integrado, que garantice una coordinación entre la regulación del Decreto Legislativo n. 231/2001 y la normativa en materia de privacidad.

The need to ensure adequate protection against the risks of unlawful data processing from virtual space has highlighted the close link between cybercrime and privacy, inducing the European legislator to promote prevention, by encouraging the adoption of effective means to protect personal data in networks and computer systems. The GDPR adopts a new risk-based approach, highlighting how the unlawful data processing is not the result of the conduct of the individual, but derives from a precise business policy. This leads to question the possibility of constructing and adopting an integrated organizational model that guarantees coordination between the provisions of Legislative Decree no. 231/2001 and the legislation on privacy.

[*] Si ringraziano i Prof.ri Antonino Gullo e Roberto Flor per i preziosi suggerimenti e gli Avv.ti Marco Ferrante e Maria Valeria Feraco, esperti in materia di *privacy*, per gli innovativi spunti di riflessione forniti.

Sommario

1. "La *privacy* nel mondo di *internet*: una nuova sfida".

«*Internet, il più grande spazio pubblico che l'umanità abbia conosciuto, la rete che avvolge l'intero pianeta*»[1].

In questo grande spazio pubblico, potenzialmente incontrollato, i giuristi si trovano continuamente di fronte a nuove sfide, alla necessità di un continuo adeguamento e ripensamento dei paradigmi e delle categorie tradizionali del diritto e all'esigenza, sempre più pressante, di garantire la tutela dei diritti fondamentali della persona, anche nel mutato contesto tecnologico.

Difatti, l'irrompere della tecnologia informatica ha messo in evidenza, da un lato, la potenzialità di tale fenomeno, e dall'altro lato, la vulnerabilità dei fruitori dello stesso, completamente esposti in rete[2].

Il processo di trasformazione digitale ha, infatti, investito la maggior parte delle relazioni tra persone, imprese e pubbliche amministrazioni[3]. La rete è ormai divenuta la nuova dimensione in cui si svolge e si esprime la personalità umana.

Con specifico riferimento alla *privacy,* la rete rappresenta per molti versi uno strumento di libertà, ma spesso determina anche un'invasione nelle sfere più intime dell'individuo. Oggi non vi è attività pubblica o privata che, essendo fondata su tecnologie, non sia anche alimentata da dati personali.

Il passaggio all'*Internet of things*, che rende oggetti comuni strumenti di connessione interattiva, ha digitalizzato ogni aspetto della vita quotidiana, moltiplicando esponenzialmente il volume dei dati personali trattati[4].

Si può osservare come i dati personali circolino in rete senza alcun filtro: basti pensare che il funzionamento e la crescita del *web* e dei *social network* si fondi soprattutto sulla registrazione, attraverso gli stessi, di una grande quantità di informazioni personali e non, acquisite anche dagli altri utenti, i quali, proprio grazie a queste tecnologie, gestiscono una vera e propria rete di contatti, che consente loro di acquisire, registrare e diffondere informazioni di varia natura, anche riferite a terzi.

Nella maggioranza dei casi tali dati sono forniti volontariamente dal titolare, ma, molto spesso, vengono fagocitati dalla rete e rimangono nella stessa, che li diffonde anche laddove il titolare non abbia prestato il consenso o non ne sia neppure a conoscenza[5].

Ne deriva l'esigenza pressante di tutelare i dati personali in rete, tentando di garantire il rispetto della dignità, dell'identità e della riservatezza della persona[6]. In questo contesto garantire la tutela dei dati personali significa «*coniugare tecnologia e umanità, libertà e sicurezza, trasparenza del pubblico e riservatezza del privato, informazione e dignità, iniziativa economica e autonomia individuale, scienza e libertà dal determinismo*»[7].

Punto di riferimento in tal senso è l'art. 8 della Carta dei diritti fondamentali dell'Unione Europea, a mente del quale il trattamento dei dati deve avvenire secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. La norma in esame individua il diritto alla protezione dei dati

[1] Rodotà, (2010), p. 338
[2] Può evidenziarsi, peraltro, come l'evolversi dell'*Information tecnology* abbia creato anche ulteriori diritti da protegge quali il diritto all'oblio o la "riservatezza informatica", quale autonomo bene giuridico ed, anzi, diritto fondamentale della persona, da intendere come diritto ad uno spazio informatico esclusivo, che a prescindere dai contenuti che vi siano presenti, trattati o comunicati, deve essere lasciato libero da intrusioni manomissioni di terzi, in quanto strumento essenziale per la piena realizzazione della persona nell'odierna vita individuale e sociale.
[3] Soro, (2018), p. 11
[4] Soro, (2018), p. 13.
[5] Galdieri, (2012), p. 2699.
[6] Pizzetti, (2010), p. 62, ha affermato che «*non si vive senza lasciare tracce della propria esistenza e, dunque, senza "produrre" dati*».
[7] Soro, (2018), p. 13.

come un diritto autonomo rispetto al rispetto della vita privata e familiare e al domicilio[8].

Similmente, l'art. 1, comma 1, D.Lgs. 30 giugno 2003, n. 196 – c.d. Codice in materia di protezione dei dati personali, come modificato dal D.Lgs. n. 10 agosto 2018, n. 101- dispone che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

Può ricordarsi, peraltro, che anche la Dichiarazione dei diritti in *internet*, documento fondamentale per garantire a ciascun individuo l'esercizio di una cittadinanza digitale attiva nel rispetto della libertà, della dignità e della diversità di ogni persona, agli artt. 5 e 6 si occupa di *privacy*, esprimendo principi, che ricalcano quelli sopra menzionati contenuti nella CEDU e nel D.Lgs. n. 196/2003, evidenziando così la stretta connessione tra rete e trattamento dei dati personali[9].

Peraltro, si osservi come il mutato contesto digitale impone un ripensamento del concetto di *privacy*, intesa non come diritto alla non divulgazione dei propri dati, ma come diritto a una corretta diffusione e gestione degli stessi. La *privacy*, comunemente intesa nell'accezione minimale di *right to be let alone,* vede «*mutare il suo contenuto da diritto alla riservatezza a diritto all'autodeterminazione informativa*»[10], arricchendosi di un contenuto ulteriore «*non solo ius excludendi alios dalla conoscenza di informazioni private, ma altresì diritto positivo al controllo dei propri dati personali*»[11]. Viene in rilievo, quindi, la proiezione sociale del diritto alla *privacy*, quale diritto non tanto alla segretezza, ma al controllo dei propri dati personali in rete e alla diffusione consapevole degli stessi[12].

Pertanto, una componente fondamentale della tutela della *privacy* diviene il diritto dell'interessato di accedere ai dati che lo riguardano e di ottenerne la rettifica ed è proprio l'aggiornamento e la contestualizzazione delle informazioni la chiave di volta per garantire una corretta rappresentazione della realtà della persona[13]. È evidente come tali attività di controllo, verifica e aggiornamento risultino particolarmente complesse in rete, in quanto mancano i riferimenti circa il luogo di conservazione dei dati e chiarezza sui criteri utilizzati per selezionarli e analizzarli, emergendo una forte asimmetria tra chi li fornisce e chi effettivamente li utilizza.

Il diritto alla *privacy*, pertanto, non può essere confinato in una sfera statica, ma la sua tutela va adeguata al «*processo evolutivo incrementale in cui si snoda la costruzione della persona*»[14], processo oggi connotato dal sempre maggiore sviluppo delle nuove tecnologie e dalla digitalizzazione di moltissimi aspetti della vita umana.

2. "L'approccio preventivo nel trattamento dei dati personali: la *privacy by design* e la *privacy by default*".

In questo scenario, stante la potenziale incontrollabilità dei dati personali una volta collocati in rete, la tutela della *privacy* si sostanzia principalmente nella necessità di prevenire un

[8] Balducci Romano, (2015), pp. 1619 ss.; Rossi Dal Pozzo, (2016), pp. 690 ss.

[9] Il testo individua una serie di principi generali che abbracciano le diverse tematiche connesse all'uso di internet: il diritto alla conoscenza e all'educazione in Rete, la neutralità della Rete, il diritto all'identità. La Dichiarazione è fondata sul pieno riconoscimento di libertà, eguaglianza, dignità e diversità di ogni persona. La garanzia di questi diritti è condizione necessaria per assicurare il funzionamento democratico delle Istituzioni. L'Art. 5. (Tutela dei dati personali), dispone che «*1. Ogni persona ha diritto alla protezione dei dati che la riguardano, per garantire il rispetto della sua dignità, identità e riservatezza. 2. Tali dati sono quelli che consentono di risalire all'identità di una persona e comprendono anche i dati dei dispositivi e quanto da essi generato e le loro ulteriori acquisizioni e elaborazioni, come quelle legate alla produzione di profili 3. Ogni persona ha diritto di accedere ai dati raccolti che la riguardano, di ottenerne la rettifica e la cancellazione per motivi legittimi 4. I dati devono esser trattati rispettando i principi di necessità, finalità, pertinenza, proporzionalità e, in ogni caso, prevale il diritto di ogni persona all'autodeterminazione informativa. 5. I dati possono essere raccolti e trattati con il consenso effettivamente informato della persona interessata o in base a altro fondamento legittimo previsto dalla legge. Il consenso è in via di principio revocabile. Per il trattamento di dati sensibili la legge può prevedere che il consenso della persona interessata debba essere accompagnato da specifiche autorizzazioni. 6. Il consenso non può costituire una base legale per il trattamento quando vi sia un significativo squilibrio di potere tra la persona interessata e il soggetto che effettua il trattamento. 7. Sono vietati l'accesso e il trattamento dei dati con finalità anche indirettamente discriminatorie*». L'art. 6. (Diritto all'autodeterminazione informativa) del medesimo provvedimento prevede che «*1. Ogni persona ha diritto di accedere ai propri dati, quale che sia il soggetto che li detiene e il luogo dove sono conservati, per chiederne l'integrazione, la rettifica, la cancellazione secondo le modalità previste dalla legge. Ogni persona ha diritto di conoscere le modalità tecniche di trattamento dei dati che la riguardano. 2. La raccolta e la conservazione dei dati devono essere limitate al tempo necessario, rispettando in ogni caso i principi di finalità e di proporzionalità e il diritto all'autodeterminazione della persona interessata*»

[10] Cfr. Torre, (2004), p. 41.

[11] Cfr. D'Agostino, (2019).

[12] Picotti (2004), p. 176; Torre, (2004), p. 239; La Manuzzi, (2017), p. 22.

[13] Tampieri, (2017), pp.101 ss.

[14] Soro, (2018), p. 8

trattamento illecito degli stessi.

Tale esigenza di prevenzione, volta a garantire un'adeguata protezione degli individui dai rischi provenienti dallo spazio virtuale, ha condotto il legislatore europeo a intervenire con Regolamento (UE) 2016/679 (c.d. GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, recepito in Italia dal citato D.Lgs. n. 101/2018, che, come anticipato, modifica il D.Lgs. n. 196/2003[15].

Innanzitutto, può osservarsi, come l'Unione Europea, attraverso l'emanazione di un Regolamento in materia di *privacy*, abbia voluto riconoscere una tutela universale della protezione dei dati personali, prevedendo diritti uniformi per tutti i cittadini europei.

Dall'individuazione della protezione dei dati personali come diritto fondamentale ne deriva il passaggio da una tutela prevalentemente rimediale, a un'essenzialmente preventiva, basata sulla responsabilizzazione dei titolari del trattamento.

Il Regolamento si caratterizza, infatti, per un mutamento di ottica, emancipandosi dagli schemi riduttivi del mercato, per accedere a una tutela più ampia della *privacy*, considerata come diritto fondamentale e protetta tramite un approccio fondato sui principi di prevenzione e precauzione[16].

Ciò che connota maggiormente le nuove previsioni contenute nel GDPR è proprio la valorizzazione del momento della prevenzione, incentivando l'adozione di efficaci misure di protezione dei dati personali, soprattutto nelle reti e nei sistemi informatici.

Tale mutamento di paradigma può ravvisarsi, *in primis*, nell'art. 25 del GDPR, che introduce i concetti di *privacy by design*, a mente del quale la protezione dei dati personali deve essere garantita sin dalla progettazione di un processo aziendale e di *privacy by default*, il quale sottintende il fatto che la protezione dei dati personali sia garantita per impostazione predefinita. Ne deriva che le tutte le valutazioni, che il titolare del trattamento deve effettuare in tema di protezione dei dati personali, devono essere compiute a monte, cioè prima di procedere al trattamento dei dati vero e proprio.

Tale norma va letta in combinato disposto con il considerando n. 78 del GDPR, a mente del quale «*la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita*».

Risulta di particolare interesse anche il principio di *accountability*, in virtù del quale i soggetti gravati dagli obblighi del GDPR dovranno autoresponsabilizzarsi e adottare precise strategie volte ad assicurare la tutela dei dati personali, avendo soprattutto riguardo ai rischi di trattamento illecito degli stessi. In dettaglio, l'art. 24 del GDPR dispone che «*tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*»[17]. Si evince come il legislatore europeo abbia abrogato le misure minime idonee previste dal vecchio art. 33, D.Lgs. n. 196/2003, sostituendole con "*misure tecniche e organizzative*", che impongono di proteggere i dati secondo modalità adeguate al caso concreto. In particolare, l'art. 32, GDPR, rubricato "*sicurezza del trattamento*", prevede che «*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative ade-*

[15] Per un'analisi delle innovazioni apportate con la riforma in parola, tra gli altri, D'Agostino, (2019), 1 ss.; D'Onofrio e T. & Macculi, (2018), pp. 1838-1841; Costantini, (2018), pp. 545-555; Castellaneta, (2018), pp. 259-265; Cuffaro (2018), pp. 1181-1185; Fronticelli Baldelli, (2018), pp. 3109-3114.

[16] Soro, (2018), p. 20; Piraino, (2017), pp. 369 ss.; Senigaglia, (2017), pp. 1023 ss.

[17] La Manuzzi (2017), p. 247; Soro, (2018), 5 ss. La responsabilizzazione viene, altresì, perseguita dal legislatore europeo tramite la cifratura - una tecnica che rende i dati incomprensibili a chiunque non sia autorizzato ad accedervi e consiste nel convertire, in maniera apparentemente casuale una sequenza di numeri e segni che solo chi ha la chiave per decifrare potrà convertire - e la pseudonimizzazione dei dati ovvero un processo, che consente di trattare i dati in maniera tale da non poterli più attribuire ad un utente in particolare senza l'accostamento di informazioni aggiuntive; la valorizzazione del ruolo di controllo e monitoraggio dell'Autorità di sorveglianza; la gestione della procedura di *data breach,* volta anche a informare l'interessato della possibile violazione dei propri dati personali.

guate per garantire un livello di sicurezza adeguato al rischio»[18]. Il livello di sicurezza e misure di protezione non è predeterminato *ex ante*, dovendo piuttosto essere adeguato al caso concreto. Il Regolamento introduce, quindi, accanto al concetto di idoneità quello di adeguatezza e, se è vero che le misure di sicurezza devono essere adeguate al livello di sicurezza e, a sua volta, quest'ultimo deve essere adeguato al rischio, è chiaro che la sicurezza di ciascun tipo di trattamento del dato personale parte dall'analisi di rischio.

Analizzato ed individuato il rischio di distruzione, perdita, modifica, divulgazione non autorizzata ovvero accesso, in modo accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati, il livello di sicurezza è adeguato quando è in grado di prevenire il rischio attraverso, appunto, misure di sicurezza idonee a mantenerlo entro una soglia di accettabilità.

Si delinea, in definitiva, un *risk based approach*, che impone alle aziende di dotarsi di misure di *compliance* tecniche e organizzative, atte a garantire un adeguato livello di sicurezza dei dati personali, facendo particolare attenzione ai rischi che connotano il trattamento.

Tale approccio preventivo pare particolarmente rilevante laddove i dati personali siano trattati in *internet,* in quanto la garanzia del consenso e dell'informativa si relativizza, atteso che la rete, per le sue dimensioni e le modalità di trattamento, si connota per la frammentazione del processo di gestione di dati, che facilmente sfugge al controllo individuale.

3. "Reati cibernetici e reati *privacy* impropri a confronto".

Il sopra descritto approccio preventivo ha posto in evidenza come il trattamento illecito dei dati personali non sia frutto della condotta del singolo, ma derivi da una precisa politica di impresa e ha fatto, quindi, emergere la necessità per le società, che inevitabilmente trattano dati personali in tutti i settori della loro attività, di attuare misure specifiche di *compliance* preventive, idonee a garantire la sicurezza dei dati. Difatti, i sopra richiamati principi di *privacy by design* e *privacy by default*, nel richiedere che la protezione del dato personale sia assicurata *ab origine,* come se fosse un'impostazione predefinita, sembrano prodromici a un'estensione dell'autoresponsabilità in ogni fase della vita dell'impresa[19].

Peraltro, ciò che caratterizza l'attività di impresa è il trattamento e coordinamento di un gran numero di dati, comuni e sensibili[20], non solo dei propri dipendenti, ma spesso anche di terzi quali agenti, fornitori, clienti e professionisti.

Tale circostanza sembra essere tenuta in considerazione dal legislatore europeo, che nel Regolamento n. 679/2016 inserisce numerose disposizioni indicative della volontà di imporre gli obblighi di corretta gestione dei dati direttamente in capo alle società.

Significativi in tal senso sono gli obblighi gestionali e organizzativi di cui al Capo IV del GDPR attuabili solo all'interno di un ente che predisponga un'adeguata politica aziendale in tal senso.

Negli stessi termini, può richiamarsi l'apparato sanzionatorio previsto dal GDPR, che sembra essere stato concepito avendo a mente la capacità economica delle grandi imprese, visti i limiti edittali così elevati nel massimo.

A ciò si aggiunga che la gestione dei dati personali confluisce nelle materie soggette a *disclosure* nella dichiarazione non finanziaria cui sono tenuti alcuni tra i cc.dd. enti di interesse pubblico[21], ai sensi del D.Lgs. n. 30 dicembre 2016, n. 254, che ha recepito la Direttiva 2014/95/UE sugli obblighi di «*comunicazione di informazioni di carattere non finanziario e di informazioni sulla diversità da parte di talune imprese e di taluni gruppi di grandi dimensioni*»[22].

Tale disposizione normativa prevede che gli enti interessati debbano comunicare le c.d. informazioni non finanziare legate, in generale, agli impatti sociali e ambientali delle azioni dell'impresa, al rispetto dei diritti umani e delle pari opportunità, alla gestione del personale

[18] Cavallari, (2018), pp. 3 ss.
[19] Bolognini, *et al.*, (2016), p. 324.
[20] Può osservarsi come le società non si limitino a trattare dati comuni dei propri dipendenti, ma ricevano anche una grande quantità di dati personalissimi e sensibili attinenti alla partecipazione ai sindacati, ad aspetti giudiziari e penali ecc.
[21] La previsione riguarda obbligatoriamente gli enti di interesse pubblico con oltre 500 dipendenti e che abbiano superato almeno uno dei due seguenti limiti dimensionali: a) totale dello stato patrimoniale: € 20.000.000; b) totale dei ricavi netti delle vendite e delle prestazioni: € 40.000.000. Per le aziende non ricadenti nell'obbligo fissato dal Decreto in parola, è ammessa la possibilità di pubblicare Dichiarazioni di carattere non finanziario su base volontaria
[22] Per un commento sul tema Bellisario, (2017), pp. 19-46; Rimini, (2018), pp. 187-199; Bonfanti, (2018), pp. 169-192; Del Prete e Ricci, (2017), pp. 509-518.

e alla lotta alla corruzione e, quindi, anche alle *policy* relative alla tutela dei dati personali[23].

Ne deriva che la normativa sui dati personali è divenuta una delle parti centrali della *compliance* societaria.

Il concetto di prevenzione, rischio e adeguatezza e la sua attuazione da parte delle imprese, inevitabilmente richiama un'assonanza con la disciplina di cui al D.Lgs. 8 giugno 2001, n. 231, sulla responsabilità amministrativa da reato delle persone giuridiche e ne fa emergere la connessione con la normativa in materia di trattamento dei dati personali.

Come noto, i reati in materia di *privacy* esulano dall'ambito applicativo del D.Lgs. n. 231/2001[24].

Un tentativo di riavvicinamento delle due discipline vi era stato tramite il decreto legge 14 agosto 2013, n. 93, recante «*Disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province*», il cui art. 9 aveva apportato, tra l'altro, una significativa modifica all'art. 24 *bis*, D.Lgs. n. 231/2001, includendo nel catalogo dei reati presupposto le seguenti fattispecie: art. 640 *ter* c.p. (frode informatica); art. 55, comma 9, del d.lgs. 21 novembre 2007, n. 231 (utilizzo indebito e falsificazione di carte di credito); artt. 167, 168 e 170 del D. Lgs. 196/2003 (illecito trattamento di dati, falsità nelle dichiarazioni e notificazioni al Garante, e inosservanza di provvedimenti del Garante).

Detta modifica legislativa sorgeva dall'esigenza di recepire le indicazioni europee e internazionali, e, in specie, la Convenzione di Budapest del 2008, che, non solo aveva imposto agli Stati Membri la produzione di una normativa tale da coprire penalmente l'eventualità del compimento di *computer crimes* in tema aziendale, ma aveva anche previsto l'introduzione di una tutela simile anche per quanto riguarda il trattamento illecito dei dati personali. La riforma in parola era destinata ad avere un forte impatto nella tutela dei dati personali all'interno delle persone giuridiche, ma non è stata confermata in sede di conversione; la legge 15 ottobre 2013 n. 119 ha, infatti, soppresso il secondo comma dell'art. 9 del decreto legge[25]. La ragione va probabilmente rinvenuta nel fatto che l'introduzione nel catalogo dei reati-presupposto dei delitti in materia di *privacy* era destinata a comportare importanti riflessi sul piano operativo per le imprese, soprattutto in relazione alla responsabilità amministrativa derivante dall'illecito trattamento dei dati; novità queste troppo rilevanti per poter essere introdotte con decretazione d'urgenza.

Il D. Lgs. 101/2018 di riforma del Codice della *privacy* non ha previsto alcuna disposizione sul punto. Il legislatore delegato ha così perduto l'ennesima occasione per introdurre una tale forma di responsabilità in tale settore nel quale l'ente continua ad essere il "grande assente"[26].

Nell'attuale formulazione dell'art. 24 *bis*, D.Lgs. n. 231/2001, quindi, seppure la rubrica reciti *"Delitti informatici e trattamento illecito di dati"*, non reca alcun riferimento ai reati in materia di *privacy*, ma solo ai delitti informatici[27].

---

[23] In particolare, l'art. 3, co. 1, D.Lgs. n. 254/2016, prevede che «*La dichiarazione individuale di carattere non finanziario, nella misura necessaria ad assicurare la comprensione dell'attività di impresa, del suo andamento, dei suoi risultati e dell'impatto dalla stessa prodotta, copre i temi ambientali, sociali, attinenti al personale, al rispetto dei diritti umani, alla lotta contro la corruzione attiva e passiva, che sono rilevanti tenuto conto delle attività e delle caratteristiche dell'impresa, descrivendo almeno: a) il modello aziendale di gestione ed organizzazione delle attività dell'impresa, ivi inclusi i modelli di organizzazione e di gestione eventualmente adottati ai sensi dell'articolo 6, comma 1, lettera a), del decreto legislativo 8 giugno 2001, n. 231, anche con riferimento alla gestione dei suddetti temi; b) le politiche praticate dall'impresa, comprese quelle di dovuta diligenza, i risultati conseguiti tramite di esse ed i relativi indicatori fondamentali di prestazione di carattere non finanziario; c) i principali rischi, generati o subiti, connessi ai suddetti temi e che derivano dalle attività dell'impresa, dai suoi prodotti, servizi o rapporti commerciali, incluse, ove rilevanti, le catene di fornitura e subappalto*».

[24] Un primo tentativo volto a introdurre la responsabilità della persona giuridica in materia di *privacy*, in epoca antecedente all'entrata in vigore del D. Lgs. 231/2001, si deve alla proposta di legge AC- 2097 presentata alla Camera dei Deputati il 12 gennaio 1993, con la quale, si delineavano alcune sanzioni applicabili direttamente alla persona giuridica per illeciti riguardanti l'omessa nomina del responsabile per la protezione dei dati personali o per la lacunosa notifica della tenuta di una banca di dati che secondo alcuni avrebbero dovuto essere inflitte dal giudice penale. Si sarebbe così ottenuto un doppio beneficio: una maggiore efficacia general-preventiva della sanzione, dotata dello stigma penale e un rispetto rigoroso delle garanzie procedurali per l'ente-imputato. Sul punto Manna, (1993), p. 185; D'Agostino, (2019), p. 50.

[25] Pistorelli, (2013), p. 7; Santoriello (2015), p. 2;

[26] Cfr. D'Agostino, (2019), p. 4; Sul punto anche Sarzana, (2008), p. 1572 ss; Corasaniti e Corrias Lucente, (2009), p. 156 ss.; Beltrani, (2008), pp. 24 ss.

[27] I reati inclusi nel catalogo del D.Lgs. n. 231/2001, all'art. 24 *bis*, sono: l'accesso abusivo ad un sistema informatico o telematico (615 *ter* c.p.), l'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617 *quater* c.p.), l'installazione di apparecchiature predisposte a tal fine (617 *quinquies* c.p.), il danneggiamento di informazioni, dati e programmi informatici (635 *bis* c.p.), il danneggiamento di informazioni, dati e programmi utilizzati da Stato, ente pubblico o di altra utilità (635 *ter* c.p.), il danneggiamento di sistemi informatici o telematici (635 *quater* c.p.), il danneggiamento di analoghi sistemi di pubblica utilità (635 *quinquies* c.p.). La medesima norma al comma 2 contempla due fattispecie di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (615 *quater* c.p.) e della diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema

Non può trascurarsi, tuttavia, come quest'ultimi siano strettamente connessi alla tutela della *privacy*, atteso che il mondo virtuale rappresenta una delle principali fonti di rischio di trattamento illecito dei dati personali.

Difatti, molti dei reati informatici inseriti nel codice penale indirettamente appaiono anche volti a tutelare la *privacy*, in quanto nel proteggere l'integrità di un sistema informatico e i dati ivi contenuti, tutelano anche la riservatezza.

Parte della dottrina definisce i reati in parola "*reati privacy impropri*", ovvero fattispecie plurioffensive, volte a tutelare il bene *privacy* in modo indiretto, come se il legislatore, attraverso la tutela dell'integrità di un sistema informatico, miri anche a proteggere i dati personali ivi contenuti[28].

In un'ottica *a contrario,* altra parte della dottrina[29] colloca accanto ai reati informatici "in *senso stretto*" – connotati dalla previsione, nella fattispecie legale, di specifici elementi di tipizzazione, contenenti un esplicito riferimento alle nuove tecnologie dell'informazione o della comunicazione – i reati informatici in senso ampio o meglio i "*reati cibernetici*" ovvero tutte quelle fattispecie la cui commissione si realizzi o possa realizzarsi in rete. Emblematici, in tal senso, sarebbero proprio i reati in materia di *privacy* di cui al D.Lgs. n. 196/2003.

Il legame tra informatica e *privacy*, emerge anche avendo riguardo al concetto di trattamento illecito dei dati personali, definito all'art. 4, n. 12, Regolamento 679/2016/UE come «*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*». I casi di *data breach* elencati appaiono sovrapponibili ai reati informatici, atteso che i concetti di diffusione, distruzione o l'accesso non autorizzato ai dati personali richiamano le condotte oggetto di alcuni delitti informatici quali, esemplificativamente, il danneggiamento di informazioni o dati o anche la distruzione di un sistema informatico che contiene dati personali (art. 615 *quinques* c.p.) o la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti di cui all'art. 615 *bis*, co. 3, c.p.

Sussiste, in definitiva, una connessione, da un punto di vista logico o cronologico, tra i reati in materia di trattamento dei dati personali e quelli informatici idonei a punire comportamenti prodromici o strumentali a violazioni della *privacy*.

4. "La prevenzione del rischio *privacy* tramite il modello di *compliance* 231".

La sopra delineata connessione tra reati *privacy* e delitti informatici consente di affermare che i *cyber crimes* creano un ponte tra il modello 231 e la disciplina sulla *privacy*, in quanto nella costruzione del modello organizzativo, volto a prevenire, tra gli altri, i reati in materia informatica, occorre avere riguardo anche alla tutela dei dati personali.

Per altro verso, il sistema di organizzazione, gestione e controllo in tema di *privacy* rileva anche sulla prevenzione dei reati informatici.

Ciò conduce a domandarsi se alla *privacy* sia applicabile il modello organizzativo di cui al D.Lgs. n. 231/2001. A ben vedere i due modelli presentano diversi punti di contatto che saranno analizzati nel prosieguo.

4.1. "*Il* risk based approach".

Con specifico riferimento ai reati informatici, in particolare, il modello organizzativo 231 si fonda sulla preventiva valutazione – di solito compendiata in un documento denominato Target of Evaluation (ToE) - di ciò che deve essere protetto, e, quindi, sull'individuazione dei

informatico o telematico (art. 615 *quinquies* c.p.).

[28] Luberto, (2008), p. 900. L'Autore suggerisce altresì un'ulteriore scissione tra i reati *privacy* impropri non informatici e informatici; infatti, gli artt. 614, 615 e 615-*bis* c.p. sono posti a tutela di un concetto di riservatezza connessa alla tutela del domicilio degli individui, sottolineandone l'aspetto prettamente materialistico. Molti altri reati sono, invece, posti a tutela di beni giuridici, fra cui la riservatezza, intrinsecamente collegati con ambiti prevalentemente informatici.

[29] Patrono, (1985), pp. 557 ss.

sistemi informatici e telematici presenti in azienda. Il modello, quindi, al suo interno, conterrà la prevenzione di tutte le fattispecie di reato che abbiano origine dall'esterno della rete aziendale e, inoltre, tutti i possibili reati che possono essere compiuti dagli utenti interni della rete stessa.

Il modello organizzativo deve, poi, prevedere una parte speciale per disciplinare l'uso del sistema informatico all'interno dell'azienda, che garantisca la trasparenza delle decisioni aziendali e dei flussi informatici di dati, tramite un criterio di tracciabilità delle decisioni e delle operazioni, per impedire o almeno facilmente rintracciare l'individuazione delle condotte di illecito utilizzo delle strutture informatiche aziendali[30].

In tale ottica sarà di assoluta importanza la nomina di un amministratore di sistema e di un responsabile delle credenziali di accesso, che si occupi di tutte le attività di gestione controllo e monitoraggio delle procedure informatiche, come il controllo degli accessi e della sicurezza.

Similmente, l'obiettivo di prevenzione e responsabilizzazione contenuto nel GDPR potrebbe essere realizzato attuando uno specifico modello organizzativo di prevenzione, del tutto simile a quello predisposto ai sensi del D.Lgs. n. 231/2001. L'elemento di novità, che è stato introdotto con il Regolamento 2016/679, è il cosiddetto *Data Protection Impact Assesment* (DPIA)[31].

Il GDPR, infatti, al fine di dare attuazione ai sopra richiamati principi di *privacy by design* e *privacy by default* e nell'ottica di un approccio preventivo alla tutela dei dati personali, all'art. 35 impone una valutazione di impatto sulla protezione dei dati, al fine di determinare l'esistenza e la gravità di rischi nel trattamento.

Si impone, quindi, al titolare e al responsabile del trattamento di effettuare uno *screening* aziendale, per comprendere che tipo di dati personali vengono trattati e quali infrastrutture tecnologiche vengono utilizzate, in modo da identificare eventuali vulnerabilità e fragilità dei sistemi. Si tratta di una vera e propria mappatura dei rischi legati al trattamento dei dati personali che ha lo scopo di ottenere la piena consapevolezza dei rischi cui l'impresa è esposta così da agevolare il processo di protezione.

Le società, inoltre, dovranno adeguatamente diversificare i processi e le funzioni inerenti la *privacy* e formare adeguatamente tutti i propri dipendenti.

4.2. "Data Protection Officer *e Organismo di Vigilanza: un legame complesso".*

Ulteriore possibile punto di contatto tra la disciplina in materia di *privacy* e i modelli 231 è la previsione di strumenti di controllo e sorveglianza sulla *compliance*. In particolare, il D.Lgs. n. 231/2001 individua nell'Organismo di Vigilanza il soggetto deputato a sorvegliare sull'adeguatezza del modello e sulla sua attuazione e aggiornamento.

Si tratta di un organismo collegiale, dotato di imparzialità e indipendenza e di autonomi poteri di controllo e iniziativa, i cui compiti, ai sensi dell'art. 6, lett. b), D.Lgs. n. 231/2001 sono vigilare sul funzionamento e l'osservanza del Modello di Organizzazione, Gestione e Controllo e di curare il suo aggiornamento[32].

Similmente, il GDPR, prevede, e in alcuni casi impone, la nomina di un *Data Protection Officer* (DPO), che, al pari dell'ODV, deve possedere specifiche caratteristiche di professionalità, imparzialità e indipendenza. Il DPO può essere un soggetto interno all'azienda, ossia un dipendente del Titolare o del Responsabile del trattamento, oppure un soggetto esterno che assolve i propri compiti sulla base di un contratto di servizi[33].

L'art. 39 del GDPR affida al DPO, tra gli altri compiti, quello di sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la

[30] Saranno, quindi, esplicitati i sistemi di controllo messi in opera al fine di monitorare l'attività dei dipendenti e approfonditi aspetti quali il documentare ed impedire comportamenti illeciti come l'uso di *password* non autorizzate, detenzione o installazione di *software* non esplicitamente previsti dall'azienda, escludere la ovvia detenzione di *virus*, *spyware* di ogni genere e dispositivi atti all'interruzione di servizi o alle intercettazioni in ambito aziendale.
[31] Pisapia, (2018), pp. 105 ss.; Cadoppi, *et al.*, (2019), pp. 1019 ss.
[32] Montalenti, (2014), pp. 7-30; Paonessa, (2014), pp. 440-448; Consulich, (2015), pp. 425-467; Giuffré, (2016), pp. 233-243; Colombo, *et. al.*, (2016), pp. 844-851; Montalenti, (2017), pp. 963-995.
[33] D'Agostino, (2017), pp. 2 ss.; Frillici, Ghini, (2017), pp. 115 ss.

formazione del personale, che partecipa ai trattamenti e alle connesse attività di controllo. Devono, infatti, essere previsti controlli periodici del mantenimento dell'adeguatezza delle misure adottate anche in previsione del fatto che tecnologia, tecnica e tipologie di trattamento sono in continuo, vorticoso sviluppo.

In entrambi i casi, sia l'OdV che il DPO nella loro attività di controllo e monitoraggio segnalano eventuali violazioni, lasciando la decisione circa le misure da intraprendere alla persona giuridica, che deve auto-valutare la situazione e decidere per il meglio, nel solco della regola di autoresponsabilità e *accountability*.

Risulta evidente, quindi, come le due figure risultino in parte coincidenti, seppure non completamente sovrapponibili, per come si dirà in seguito.

A ben vedere la disciplina in materia di privacy incide sul ruolo dell'OdV anche sotto altri aspetti. In particolare, il dibattito dottrinale alla luce dell'entrata in vigore del GDPR e del D.Lgs. n. 101/2018, si è focalizzato sulla posizione dell'organismo di vigilanza rispetto agli obblighi in materia di privacy[34].

Ciò, poiché, detto organismo, nello svolgimento delle sue attività "*entra in contatto con una pluralità di dati personali, quali, in particolare, dati sensibili e dati giudiziari: ciò impone, dunque, di procedere all'individuazione dei pertinenti profili [soggettivi] connessi con il trattamento dei dati personali*"[35].

In dettaglio, l'OdV tratta dati personali provenienti dai flussi informativi, di cui all'art. 6, co. 2, lett. d), D.lgs. 231/2001 e dalle proprie attività di controllo e vigilanza.

Ulteriori dati potrebbero anche derivare dalle segnalazioni sulle violazioni del modello che l'organismo riceve in attuazione della disciplina sul *Whistleblowing*, di cui si dirà in seguito.

È evidente, quindi, come sia di estrema rilevanza stabilire quale posizione soggettiva l'OdV ricopra rispetto ai dati personali trattati e, quindi, quali siano gli obblighi in materia di *privacy* che lo stesso deve rispettare.

In *primis* occorre chiarire che l'OdV - laddove non sia monosoggettivo ma, come auspicato anche dalla Linee Guida in materia e dalla dottrina[36], sia un organismo collegiale - debba essere inteso come un *unicum*.

Difatti, come già sancito dall'art. 28 del D.lgs. 196/2003, in caso di soggetti complessi le qualifiche soggettive *privacy* devono essere riferite a "*l'entità nel suo complesso, considerando come responsabile del trattamento la società o l'organismo in quanto tali piuttosto che una specifica persona al loro interno*"[37]. Gli obblighi in materia di *privacy*, in definitiva, gravano sull'OdV inteso come entità e non sui singoli membri, interni o esterni, che lo compongono.

Punto nodale resta lo stabilire se l'organismo in parola possa essere qualificato come titolare del trattamento dei dati personali o come mero responsabile, laddove il primo viene definito dall'art. 4, n. 7, GDPR come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*", mentre il secondo, ai sensi dell'art. 4, n. 8, GDPR è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*".

Parte della dottrina qualifica l'OdV come titolare del trattamento, ritenendo che dagli autonomi poteri di iniziativa e controllo, attribuiti all'organismo dall'art. 6, D.Lgs. n. 231/2001, ne derivino anche i poteri di determinare le finalità e i mezzi del trattamento propri del titolare[38].

Tale approccio non trova l'accoglimento di altra parte della dottrina che, in un'ottica funzionalista, fondata sull'attività e i poteri effettivamente attribuiti al titolare del trattamento, evidenzia come il compito di vigilare non possa essere confuso con l'autonomia nella determinazione delle finalità della vigilanza e, quindi, dei trattamenti strumentali ad essa[39].

Tale dottrina evidenzia come le finalità del trattamento dei dati di interesse dell'OdV non sono determinate dall'organismo stesso bensì: "*a) predeterminate, in generale, dal d.lgs. 231/2001 ("vigilanza sul funzionamento e l'osservanza dei modelli" per "prevenire reati della specie di quello*

[34] Sul tema si veda il *Position Paper* sulla posizione soggettiva dell'ODV a fini privacy, elaborato dall'AODV nel marzo 2019, in *www.aodv231.it*.
[35] Perinu, (2019), 2 ss.
[36] *ex multis*, Galletti, (2006), pp. 126 ss.; Montalenti, (2009), pp. 643 ss.
[37] Bolognini *et. al.*, (2016), pp. 124 ss.
[38] Perugini, (2017), pp. 2 ss.
[39] *Position Paper* sulla posizione soggettiva dell'ODV a fini privacy, elaborato dall'AODV nel marzo 2019, in *www.aodv231.it.*

verificatosi"); b) e declinate, in particolare, dal modello di organizzazione, gestione e controllo, che è "adottato [dal]l'organo dirigente" e non dall'OdV (art. 6, comma 1, lett. a), d.lgs. 231/2001); c) lo stesso OdV è istituito da "l'organo dirigente" (art. 6, comma 1, lett. b), d.lgs. 231/2001) che "dovrà disciplinare gli aspetti principali relativi al funzionamento dell'OdV"[40].

Peraltro, anche con riferimento ai mezzi che l'organismo utilizza per il trattamento, si è evidenziato come questi vengano determinati negli aspetti fondamentali dall'organo dirigente nell'ambito della disciplina del funzionamento dell'OdV.

Infine, occorre considerare che "*il rispetto delle norme al cui controllo [gli OdV] sono preposti è innanzitutto un obbligo gravante sulla società oggetto del controllo*"[41], sicché l'organismo si limita a trattare dati personali già appartenenti all'ente vigilato.

Esclusa la configurabilità dell'OdV come titolare del trattamento dei dati personali, parte della dottrina esclude anche che la qualifica di responsabile possa essere attribuibile all'organismo. Ciò alla luce delle modifiche intervenute con il GDPR e il D.lgs. n. 101/2018, che hanno escluso la possibilità che il responsabile del trattamento sia un soggetto interno all'ente. Difatti, secondo la nuova disciplina, requisito essenziale per essere riconosciuto quale responsabile è "*essere una persona giuridica distinta dal titolare*"[42], che, nel caso di specie, sarebbe l'ente vigilato dall'OdV[43].

Nel caso dell'OdV una siffatta distinzione non sarebbe configurabile, atteso che lo stesso ai sensi dell'art. 6, D.lgs. n. 231/2001, è un organismo dell'ente, interno allo stesso[44]. Peraltro, i requisiti di indipendenza e autonomia che connotano l'OdV sarebbero incompatibili con il ruolo di responsabile del trattamento, il quale agisce secondo le indicazioni fornite dal titolare, creandosi un conflitto di interessi tra controllante (l'OdV) e controllato (l'ente)[45].

In definitiva la tendenza dominante è quella di ritenere assorbito l'inquadramento soggettivo dell'OdV ai fini della *privacy* da quello dell'ente vigilato del quale l'organismo costituisce una parte[46].

Ciò, peraltro, non esclude che l'ente vigilato, in qualità di Titolare, possa prescrivere all'OdV, nell'ottica dell'attuazione del principio di *accountability*, il rispetto di particolari misure tecniche e organizzative adeguate a garantire che il trattamento sia effettuato conformemente al GDPR, purché non interferenti con gli autonomi poteri di iniziativa e di controllo spettanti all'organismo[47].

4.3. *"La disciplina del* Wisthleblowing*".*

Infine, sia il D.Lgs. n. 231/2001 sia il GDPR si occupano di *Whistleblowing*.

Per quanto concerne la responsabilità amministrativa da reato, la legge 30 novembre 2017, n. 179, recante "*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*" ha, tra l'altro, modificato l'art. 6, D.Lgs. n. 231/2001, al fine di prevedere una puntuale tutela per tutti quei dipendenti e/o collaboratori di società, che abbiano segnalato illeciti di cui siano venuti a conoscenza nell'ambito delle proprie mansioni lavorative[48].

In particolare, sono stati introdotti i nuovi commi 2 *bis*, 2 *ter* e 2 *quater* nella citata disposizione, la quale, nella formulazione attuale, dispone che i modelli organizzativi devono prevedere al loro interno una pluralità di "canali" diversi, rispetto a quello comune della *governance* prestabilito in base al diritto societario applicabile secondo la struttura prescelta, che consentano di presen-

[40] *Position Paper* sulla posizione soggettiva dell'ODV a fini privacy, elaborato dall'AODV nel marzo 2019, in *www.aodv231.it.*
[41] Perugini, (2017), pp. 2 ss.
[42] Opinion 1/2010 del Art. 29 *Data Protection Working Party*
[43] Tale soluzione non convince parte della dottrina che osserva come nei casi in cui l'OdV sia composto solo da membri esterni o abbia una composizione mista non può rivestire una posizione equiparabile a quella dell'ente ma dovrebbe essere nominato responsabile del trattamento, con obblighi di autonomi di verifica e controllo. Sul punto, Barbarossa (2019), pp. 2 ss.
[44] Santoriello, (2015), pp. 109 ss.; Pisani, (2008), pp. 155 ss.; Sfameni, (2007); Rordorf, (2001), 1297 ss.; Bartolomucci, (2002), pp. 10 ss.;
[45] Perugini, (2017), pp. 2 ss. L'OdV non potrebbe neppure rivestire la qualifica di autorizzato al trattamento riferita esclusivamente a persone fisiche, mentre l'OdV normalmente come detto è un organismo collegiale da considerare come tale anche ai fini della qualificazione *privacy*.
[46] *Position Paper* sulla posizione soggettiva dell'ODV a fini privacy, elaborato dall'AODV nel marzo 2019, in *www.aodv231.it.*
[47] Perugini, (2017), pp. 2 ss.
[48] Coceani, (2018), pp. 293-302; Frignani e Grosso, (2004), p. 387; Frignani, (2018), pp. 3 ss.; Ferrante, (2018). Pp.145-172; D'Urgolo, (2018), pp. 2 ss.

tare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del D.Lgs. n. 231/2001 o di violazioni del modello di organizzazione e gestione dell'ente[49]. La nuova disciplina impone, altresì, il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione e l'introduzione nel sistema disciplinare di sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

È previsto, altresì, che l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni possa essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo. In ultimo, l'art. 6, co. 2 *quater*, D.Lgs. n. 231/2001 dispone la nullità del licenziamento ritorsivo o discriminatorio del soggetto segnalante, così come di qualsiasi altra misura ritorsiva. Nel caso di controversie legate all'irrogazione di sanzioni disciplinari o all'adozione di ulteriori misure organizzative con effetti negativi sulle condizioni di lavoro del segnalante, il datore di lavoro ha l'onere di dimostrare che esse sono fondate su ragioni estranee alla segnalazione stessa[50].

In applicazione di detta disciplina si ritiene che il Modello Organizzativo debba indicare chiaramente a quale soggetto o organo debbano essere indirizzate le segnalazioni oggetto delle nuove disposizioni. Tale soggetto potrebbe certamente essere l'Organismo di Vigilanza in virtù della sua autonomia e indipendenza rispetto ai vertici dell'ente[51].

Sembra evidente che la disciplina del *whistleblowing* debba integrarsi con la disciplina in materia di *privacy*.

In dettaglio, il D.Lgs. n. 101/2018 ha modificato il D.Lgs. n. 196/2003, prevedendo all'art. 2 *undecies*, co. 1, lett. f), la possibilità di limitare l'esercizio dei diritti d'accesso dell'interessato nel caso in cui ne possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del dipendente, che segnala, ai sensi della legge n. 179/2017, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio[52]. La medesima norma prevede, altresì, che, nei casi in parola, l'esercizio dei diritti dell'interessato può essere limitato, ritardato o eventualmente eluso per mezzo di una comunicazione motivata, senza che questa possa in alcun modo compromettere la finalità della limitazione, nei tempi e nei limiti in cui questo rappresenti una misura proporzionata e necessaria[53].

Si noti che tanto il D.Lgs. n. 231/2001 quanto il Codice *privacy* tutelano la riservatezza dell'identità del segnalante e non il suo anonimato, richiedendo che l'identità del soggetto che segnala sia comunque nota. Come chiarito dall'Autorità Nazionale Anticorruzione, difatti, il denunciante può godere di una tutela adeguata soltanto se si rende riconoscibile[54]. Ciò non esclude che i modelli organizzativi possano contemplare anche canali per effettuare segnalazioni in forma anonima. Tale ipotesi sembra, tuttavia, rendere più complessa la verifica della fondatezza della denuncia, con il rischio di alimentare denunce infondate, che hanno poco a che fare con la tutela dell'integrità dell'ente[55].

Sul tema rilevante pare anche l'intervento della legislazione europea, attuato in data 16 aprile 2019 con la "*Risoluzione legislativa del Parlamento europeo sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*"[56]. Si tratta di un'innovazione legislativa rilevante poiché fissa *standard* minimi di protezione allo scopo di superare le diversità di trattamento esistenti fra i vari Paesi

[49] L'art. 6, co. 2 bis, D.Lgs. n. 231/2001, in dettaglio, dispone che debbano essere previsti : «*a) uno o più canali che consentano ai soggetti indicati nell'articolo 5, comma 1, lettere a) e b), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione; b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante; c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione; d) nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate*».
[50] Sul tema si vedano le Linee Guida di Confindustria sulla disciplina del *whistlebolwing*, in *www.confindustria.it*
[51] Linee Guida di Confindustria sulla disciplina del *whistlebolwing*, in *www.confindustria.it*
[52] Bolognino, (2018), pp. 9 ss.
[53] Fedi, (2018), pp. 1087 ss.
[54] Determinazione ANAC n. 6 del 28 aprile 2015, "*Linee Guida in materia di tutela del dipendente pubblico che segnala illeciti*", in *www.anticorruzione.it*
[55] Linee Guida di Confindustria sulla disciplina del *whistlebolwing*, in *www.confindustria.it*
[56] Testo consultabile in *www.eurlex.it*

europei, armonizzando la disciplina.

La Direttiva estende l'obbligo di offrire canali di ricezione delle segnalazioni sicuri a tutte le aziende con più di 50 dipendenti sia pubbliche che private e conferma l'obbligo di svolgere indagini interne, portando dunque le aziende ad assumere un comportamento più proattivo nella prevenzione e gestione degli illeciti commessi all'interno dell'ente.

Per garantire la sicurezza dei potenziali informatori e la riservatezza delle informazioni divulgate, le nuove norme consentiranno di comunicare le segnalazioni direttamente alle autorità nazionali competenti, nonché agli organi e le agenzie competenti dell'UE. Pertanto, tali canali di comunicazione dovranno essere creati sia dagli enti sia dalle autorità nazionali.

In più, fornisce una protezione legale a un ampio ventaglio di soggetti, non solo dipendenti ma anche consulenti, fornitori, stagisti e volontari.

Tale intervento legislativo certamente condurrà il legislatore italiano a introdurre nuove norme di adeguamento alla normativa europea, con conseguenti modificazioni sia in materia di *privacy* che in tema di *compliance ex* D.Lgs. n. 231/2001.

5. "Verso un nuovo modello organizzativo *privacy* integrato?"

I delineati elementi di somiglianza non devono condurre a ritenere che il modello organizzativo 231 possa essere applicato *tout court* alla disciplina in materia di *privacy,* che presenta delle particolarità. L'approccio *risk based* è sicuramente il medesimo, tuttavia, sembrano potersi ravvisare delle differenze rispetto all'oggetto e alla finalità dello stesso.

La valutazione del rischio *ex* D.lgs. 231/01, da un lato mira a rintracciare, analizzare e valutare i rischi di commissione del reato, che possono fisiologicamente annidarsi nella gestione dei processi aziendali, dall'altro lato, risulta funzionale a garantire l'integrazione e l'attuazione di misure di controllo, che consentano di pervenire ad un'organizzazione aziendale tale da prevenire la commissione di reati.

Per converso la valutazione del rischio *ex* GDPR mira a rintracciare, analizzare e valutare il rischio di trattamento illecito dei dati personali, al fine di conformarsi ad un obbligo legislativo e, contestualmente, di proteggere e tutelare l'interessato al trattamento.

Peraltro, l'esenzione di responsabilità a favore della persona giuridica di cui agli artt. 6 e 7, D.Lgs. n. 231/2001, in relazione all'esatta costruzione e applicazione del modello organizzativo, non è prevista nel GDPR, nell'ambito del quale l'adozione di un modello di *compliance* efficiente è solo un elemento di valutazione della responsabilità del titolare del trattamento. Difatti, anche l'adozione di eventuali codici di condotta certificati, pure previsti, non ha funzione scriminante, ma è semplicemente sintomo di adeguatezza delle misure adottate al GDPR.

Con riferimento, poi, alle figure del DPO e dell'OdV queste, come anticipato, non sono sovrapponibili, avendo funzioni differenti. L'OdV sorveglia il modello organizzativo "dall'esterno" senza entrare nello stesso, il DPO, invece, riveste anche una funzione consultiva, che determina una sua maggiore ingerenza nella *compliance* in materia di *privacy*. Inoltre, le valutazioni operate dal DPO hanno un riferimento positivo quale il Codice *privacy* e il GDPR, a differenza dell'OdV, che ha a riferimento il modello organizzativo e la sua adeguatezza preventiva.

Può osservarsi, tra l'altro, come le uniche condotte di reato rilevanti nell'ambito della costruzione di un modello organizzativo, ai sensi del D.Lgs. n. 231/2001, siano quelle finalizzate a portare un interesse o un vantaggio per la persona giuridica.

Difatti, prevenire il rischio di trattamento illecito dei dati *ex* D.Lgs. 231/01, a stretto rigore, significa prevenire il trattamento illecito commesso nell'interesse o a vantaggio della persona giuridica, non essendo rilevanti quelle condotte poste in essere nell'interesse o a vantaggio di terzi o addirittura dannose per l'ente.

Diversamente, il modello organizzativo *privacy* dovrebbe essere volto a prevenire tutte le ipotesi di violazione della normativa in materia, anche quelle che determinerebbero un danno per la società. Pertanto, aver implementato ed attuato un idoneo e adeguato sistema dei controlli ai sensi del D.Lgs. n. 231/2001 può non esser sufficiente per poter vantare un idoneo e adeguato sistema di protezione dei dati personali trattati.

Dalle considerazioni sopra svolte, risulta evidente come sia veramente auspicabile un intervento normativo di armonizzazione e coordinamento del coacervo di norme che disciplinano la *cyber security* di dati, sistemi e reti e i modelli di prevenzione degli illeciti nelle aziende. In

particolare, vista la forte esigenza di prevenzione nell'ambito della tutela dei dati personali in ambito societario e atteso che la tutela di cui all'art. 24 *bis*, D.Lgs. n. 231/2001 risulta debole e inidonea a ricomprendere tutte le possibili condotte lesive della *privacy,* sarebbe certamente auspicabile un intervento legislativo volto a introdurre i reati relativi al trattamento dei dati personali nell'ambito delle fattispecie presupposto di cui al D.Lgs. n. 231/2001. Il legislatore dovrebbe procedere a un'opera di coordinamento tra il modello 231 e il modello organizzativo delineato dal GDPR, evitando duplicazioni organizzative e sanzionatorie e semplificando l'attività di adeguamento delle imprese, che oggi vanno incontro a inutili appesantimenti nella gestione societaria. Ciò consentirebbe di rafforzare e rendere più efficiente la tutela dati personali trattati nel panorama aziendale e della riservatezza informatica in generale, affrontando il problema direttamente e non in modo trasversale.

In mancanza di un intervento legislativo organico, l'obiettivo verso cui tendere è l'implementazione di un sistema di controlli idoneo ed adeguato a prevenire il rischio di commissione di reati "connessi" al trattamento di dati personali, ivi inclusi i reati informatici, e, al contempo, idoneo a proteggere gli stessi dati personali dagli specifici rischi contemplati dal GDPR. Ciò che sicuramente ha preminente importanza è non creare un sistema di controlli interno ridondante e/o, addirittura, incoerente: reciprocità e relazione, ove possibili, non potranno che accrescere l'efficacia del sistema dei controlli interni aziendali.

Tale obiettivo si potrebbe realizzare con la costruzione e l'adozione di un modello organizzativo integrato, soprattutto con riferimento ai delitti informatici, che garantisca un coordinamento e collegamento tra la disciplina di cui al D.lgs. n. 231/2001 e la normativa in materia di *privacy*, tenendo conto delle peculiarità di quest'ultima.

Ciò al fine di evitare una duplicazione di procedure e di coordinare le figure di controllo, ovvero il DPO e l'OdV, che potrebbero cooperare nell'aggiornamento del modello integrato per le materie inerenti al trattamento e la protezione dei dati e i reati informatici. In particolare, il DPO, quale figura di controllo di secondo livello, dovrebbe informare periodicamente l'Organismo di Vigilanza circa i trattamenti in essere e sulla prevenzione di reati, segnalando eventuali violazioni.

L'Organismo di Vigilanza dovrebbe, invece, collaborare con il DPO, al fine di aggiornare il Modello per le materie inerenti al trattamento e la protezione dei dati e per avere informazioni sulla *privacy*, sia a livello di adempimenti normativi, sia a livello, più tecnico, di predisposizione delle sicurezze per il corretto trattamento.

Tale modello integrato potrebbe rendere più effettiva la compliance in un'ottica principalmente preventiva, con l'obiettivo di incrementare la tutela dei dati personali nell'ambito delle realtà d'impresa e di responsabilizzare maggiormente non solo i singoli, ma soprattutto le persone giuridiche.

Ciò fermo restando che si potrà giungere ad una tutela effettiva dei dati personali in rete solo tramite la diffusione di una cultura della protezione dei dati personale, fondata sulla comprensione del fatto che la *privacy* non è un costo per le società, sempre più digitali e interconnesse, ma una risorsa essenziale da proteggere.

Quella della protezione dei dati è ormai divenuta una frontiera su cui si gioca una parte rilevante del nostro futuro come singoli e come collettività. Pertanto, per le persone giuridiche «*il passo più importante che resta da fare, raccogliendo una delle sfide più importanti che il legame tra tecnologica, diritti e prevenzione pone alle nostre generazioni, è quello del riconoscimento universale del diritto alla protezione dei dati personali, quale primo presupposto di libertà nel XXI secolo*»[57].

Bibliografia

Balducci Romano, Fabio, (2015), "La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo", *Rivista italiana di diritto pubblico comunitario*, 6, pp. 1619-1659;

Bartolomucci, Sandro (2002), "Responsabilità amministrativa dell'ente: l'adozione di modelli organizzativi", *Diritto e pratica societaria*, 17, pp. 10-25;

[57] Soro, (2018), p. 166

Bellisario, Elena (2017), "Rischi di sostenibilità e obblighi di "disclosure": il d. lgs. n. 254/16 di attuazione della dir. 2014/95/UE", *Le Nuove leggi civili commentate*, 1, pp. 19-46;

Beltrani, Sergio, (2008), Reati informatici e d.lgs. 231/2001 alla luce della legge di attuazione della Convenzione di Budapest, *La responsabilità amministrativa delle società e degli enti*, 2008, 4, pp. 24 ss.

Bolognini, Luca, Pelino, Enrico, Bistolfi, Camilla, (2016), *Il Regolamento privacy europeo*, (Milano, Giuffrè).

Bonfanti, Angelica, (2018), "Corporate social responsibility and corporate accountability: the Italian private international law perspective", *Annuario di diritto comparato e di studi legislativi*, pp. 169-192;

Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo, (2019), *Cybercrime*, (Milano, Ipsoa);

Castellaneta, Marina (2018), "L'incidenza del regolamento GDPR sul quadro normativo esistente", *Notariato*, 3, pp. 259-265;

Cavallari, Giulia (2018), La sicurezza del trattamento: analisi dell'articolo 32 GDPR, *www.iusinitinere.it*;

Coceani, Michele, (2018), "Whistleblowing" nel settore privato e sicurezza sul lavoro", *ISL: igiene e sicurezza del lavoro*, 5 pp. 293-302;

Colombo, Cristina, Maniccia, Alessia, Tescione, Vincenzo, (2016), "L'organismo di vigilanza ex d.l.vo n. 231/01. Requisiti, funzioni e profili problematici", *Rivista penale*, 10, pp. 844-851;

Consulich, Federico (2015), "Vigilantes puniri possunt". I destini dei componenti dell'organismo di vigilanza tra doveri impeditivi e cautele relazionali, *Rivista trimestrale di diritto penale dell'economia*, 3, pp. 425-467;

Corasaniti, Giuseppe, Corrias Lucente, Giovanna, (2009), *Cybercrime, responsabilità degli enti, prova digitale*, (Padova, Cedam);

Costantini, Federico, (2018), "Il Regolamento (UE) 679/2016 sulla protezione dei dati personali", *Il Lavoro nella giurisprudenza*, 6, pp. 545-555;

Cuffaro, Vincenzo, (2018), "Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati Commento a d.lg. 10 agosto 2018, n. 101", *Corriere giuridico*, 10, pp. 1181-1185;

D'Agostino, Luca, (2019), "La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101", *Archivio penale*, 1-58;

Del Prete, Chiara, Ricci, Daniela, (2017), "Comunicazione di informazioni di carattere non finanziario e di informazioni sulla diversità. D.Lgs. n. 254/2016: introduzione alla disciplina e problematiche applicative", *Rivista dei dottori commercialisti*, 4, pp. 509-518.

D'Onofrio, Tommaso, Macculi, Carlo, (2018), "La rivoluzione GDPR", *Corriere tributario*, 23, pp. 1838-1841;

D'Urgolo, Giandomenico, (2018), "La tutela del pubblico dipendente (e non solo) che segnala illeciti (c.d. "whistleblower")", *GiustAmm.it*, 3, pp. 1-7;

Fedi, Andrea, (2018), "Diritti dell'impresa e protezione dei dati personali", *Le Società*, 10, pp. 1087-1100;

Ferrante, Vincenzo, (2018), "Novità per il settore pubblico e privato in tema di "whistleblowing", *Il lavoro nel diritto*, 2, pp. 145-172;

Frignani, Aldo, (2018), "Whistleblowing": finalmente una legge generale "ad hoc". Luci ed ombre", *Nuovo notiziario giuridico* pp. 1-20;

Frignani, Aldo, Grosso, Patrizia, (2004), L'organismo di controllo, sua composizione e problematiche, Monesi, Carlo, (eds.), *Modelli organizzativi ex d.lgs. 231/2001 (Etica d'impresa e punibilità degli enti)*, (Giuffrè, Milano), pp. 387;

Frillici, Alessandro, Ghini, Patrizia, (2017), La figura del DPO, Rivista 231, pp. 115 ss.;

Fronticelli Baldelli, Enrico (2018), "In vigore il Decreto in materia di Privacy", *Corriere tributario*, 40, pp. 3109-3114;

Galdieri, Paolo, (2012), "Il trattamento illecito del dato nei "social network", in *Giurisprudenza di merito,* 2012, 12, pp. 2699 ss.;

Galletti, Danilo, (2006), "I modelli organizzativi nel d.lgs. n. 231/2001: le implicazioni per la corporate governance", *Giurisprudenza Commentata*, 126-146;

Italiano", *Rivista trimestrale di diritto penale dell'economia,* 1, pp. 185 ss.;

La Manuzzi, Marta, (2017), Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE, *JusOnli-ne,* 1, pp. 218-265;

Luberto, Mario, (2008), "I reati informatici contro il diritto alla privacy. La tutela fornita dal D.lgs 196 del 2003 e dal codice penale", *Giurisprudenza di merito,* 3, pp. 898 ss.;

Manna, Adelmo, (1993*),* "La protezione personale dei dati personali nell'ordinamento

Montalenti, Paolo (2014), "Modello "231" e organismo di vigilanza nel sistema dei controlli societari: un quadro d'insieme", *Il Nuovo Diritto delle Società*, 2, pp. 7-30;

Montalenti, Paolo (2017), "Prevenzione dei reati tributari (c.d. "Cooperative Compliance"), Modello 231, sistemi di controllo e "governance" societaria: profili generali e ipotesi di riforma", in *Il Nuovo Diritto delle Società*, 9, pp. 963-995;

Montalenti, Paolo, (2009), Organismo di vigilanza e sistema dei controlli, *Giurisprudenza Commentata*, I, 643- 660;

Paonessa, Caterina (2014), "Il ruolo dell'organismo di vigilanza nell'implementazione dei modelli organizzativi e gestionali nella realtà aziendale", *La Giustizia penale*, 7, pp. 440-448;

Patrono, Paolo, (1985), "Privacy e vita privata", Enciclopedia del Diritto, XXXV, pp. 557 ss.;

Perinu, Paola (2019), La privacy e la vigilanza sul modello 231. Quale ruolo per l'Organismo di Vigilanza?, *www.AOdV231.it,* pp. 1-6;

Perugini, Maria Roberta (2017), "Organismi di vigilanza e controllo e ruoli privacy: valutazioni generali e prime considerazioni sui trattamenti del DPO", in *https://europrivacy.info.it/2017/01/09*;

Picotti, Lorenzo, (2004), "Reati informatici, riservatezza, identità digitale", *www.aidp.it*, pp. 1-18;

Piraino, Fabrizio (2017), "Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato", *Nuove leggi civile commentate*, 2017, pp. 369-409;

Pisani, Nicola, (2008), I requisiti di autonomia ed indipendenza dell'organismo di vigilanza istituito ai sensi del d.lgs. 231/2001, *La responsabilità amministrativa delle società e degli enti*, 1, pp. 155 ss;

Pisapia, Alice (2018), *La tutela per il trattamento e la protezione dei dati personali,* (Torino, Giappichelli);

Pistorelli, Luca (2013), Relazione Ufficio del Massimario Cassazione, n. III/01/2013 del 22 agosto 2013, p. 7;

Pizzetti, Franco, (2010), "La tutela della riservatezza nella società contemporanea", *Percorsi costituzionali*, I, pp. 62 ss.

Position Paper sulla posizione soggettiva dell'ODV a fini privacy, elaborato dall'AODV nel marzo 2019, in *www.aodv231.it.*

Rimini, Emanuele, (2018), "I valori della solidarietà sociale nelle dichiarazioni non finanziarie", *Analisi giuridica dell'economia*, 1, pp. 187-199;

Rodotà, Stefano, (2010), "Una costituzione per internet?", *Politica del diritto*, 3, pp. 337-351;

Rordorf, Renato, (2001), I criteri di attribuzione della responsabilità. I modelli organizzativi e gestionali idonei a prevenire reati, *Le società*, 11, pp. 1297 ss.;

Rossi Dal Pozzo, Francesco, (2016), "La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal safe harbour al privacy shield)", *Rivista di diritto internazionale,* pp. 690 ss.

Santoriello, Ciro, (2015), Attività dell'organismo di vigilanza e obbligo di segretezza in capo ai suoi componenti, *La responsabilità amministrativa delle società e degli enti*, 4, pp. 109 ss.

Sarzana, Carlo, (2008), "La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa", *Diritto penale e processo,* 12, pp. 1572 ss

Senigaglia, Roberto, (2017), "Reg. Ue 2016679 e diritto all'oblio nella comunicazione telematica - Identità, informazione e trasparenza nell'ordine della dignità personale", *Nuove leggi civili*, 2017, pp. 1023 ss.

Sfameni, Paolo, (2007), "Responsabilità da reato degli enti e nuovo diritto azionario: appunti in tema didoveri degli amministratori ed organismo di vigilanza", *Rivista delle società*, 1, 2007, 183.

Soro, Antonello, (2018), "Persona, diritti e Innovazione", Relazione Garante privacy, pp. 1-16 ss.

Tampieri, Maura, (2017), Il diritto all'oblio e la tutela dei dati personali, *Responsabilità Civile e Previdenza*, 3, pp. 101 – 137;

Torre, Valeria, (2004), La gestione del rischio nella disciplina del trattamento dei dati personali, in Picotti Lorenzo (eds.), Il diritto penale dell'informatica nell'epoca di internet, (Padova, Cedam), pp. 237-277.

Sicurezza informatica, compliance e prevenzione del rischio di reato

Seguridad informática, compliance y prevención del riesgo de delitos

IT Security, Compliance and Crime Prevention

I discorsi d'odio nell'era digitale: quale ruolo per l'internet service provider?

Los discursos de odio en la era digital: ¿Cuál es el rol del proveedor de servicios de internet?

Hateful Speech in the Digital Era: Which Role for the ISP?

Valérie Nardi
Dottoressa di ricerca in "Scienze Giuridiche - Tutela penale e garanzie della persona nel diritto interno, comparato, europeo ed internazionale: profili sostanziali e processuali presso l'Università degli Studi di Messina
vnardi@luiss.it

Libertà di espressione, Diffamazione
Libertad de expresión, Difamación
Freedom of expression, Defamation

Abstracts

L'evoluzione degli strumenti di comunicazione digitale e, soprattutto, l'affermazione dei social network hanno aperto la strada ad una pervasiva proliferazione dei discorsi d'odio in rete. Al fine di ostacolare la propagazione delle opinioni discriminatorie e non rispettose della dignità umana, risulta quanto mai rilevante la definizione del ruolo e delle eventuali responsabilità degli intermediari informatici, stante il contributo che gli stessi apprestano alla diffusione e alla permanenza in rete dei contenuti digitali, ma, soprattutto, in quanto principali soggetti in grado di rimuovere materialmente i messaggi illeciti. Occorre, tuttavia, verificare se l'approccio punitivo – e, più specificamente, il ricorso alla sanzione penale – sia davvero il più ragionevole, considerati i rischi che una tendenza repressiva potrebbe implicare rispetto alla libertà di espressione degli utenti e alla libertà di impresa dei *provider*.

La evolución de los instrumentos de comunicación digital y, sobre todo, la expansión de las redes sociales han tenido como consecuencia una proliferación de los discursos de odio en línea. A fin de obstaculizar la propagación de opiniones discriminatorias y no respetuosas de la dignidad humana, resulta relevante la definición del rol y de las eventuales responsabilidades de los intermediarios informáticos, dada su contribución a la difusión y permanencia del contenido digital en la red, pero, sobre todo, como los principales sujetos capaces de eliminar materialmente mensajes ilícitos. Sin embargo, es necesario verificar si el enfoque punitivo, especialmente la utilización de sanciones penales, sea en realidad el más razonable, considerando los riesgos que una tendencia represiva podría significar en relación a la libertad de expresión de los usuarios y a la libertad de empresa del proveedor de servicios de internet.

The IT communication evolution and, even more, the key-role played by social networks facilitated the spread of hateful speech on-line. In order to avoid the dissemination of discriminatory opinions, not respectful for human dignity, it is crucial defining the role and the liability, if any, of IT intermediaries, in light of the contribution they give to spreading and hosting of on-line content, especially since they are the only ones who can practically remove unlawful messages. It is worth, however, checking if the punitive paradigm – and, more in detail, criminal sanctions – is the fairest, considering also the risk that repression would imply with respect to the freedom of expression and business freedoms of providers.

Sommario

1. Premessa: fenomenologia dei discorsi d'odio 2.0.

Sebbene si tratti di un termine molto diffuso, anche in ambito giuridico, l'*hate speech* – o discorso d'odio – non è ad oggi oggetto di una descrizione universalmente condivisa[1]. Secondo un'apprezzabile operazione di sintesi, elaborata in riferimento al "discorso razzista", ma applicabile in genere a tutte le categorie potenziali destinatarie di parole odiose, l'*hate speech* può essere definito come quel «discorso finalizzato a promuovere odio nei confronti di certi individui o gruppi, impiegando epiteti che denotano disprezzo nei confronti di quel gruppo a causa della sua connotazione razziale, etnica, religiosa, culturale o di genere»[2].

Si tratta, evidentemente, di un fenomeno affatto nuovo, che anzi molto spesso costituisce la riproposizione in forma linguistica di un rapporto di emarginazione e subordinazione esistente – o esistito – nei confronti di taluni classi di persone, contrassegnate nel contesto storico-sociale di appartenenza da una qualche ragione minorante[3]. L'effetto è quello di alimentare i pregiudizi, consolidare gli stereotipi e rafforzare l'ostilità, fino a identificare l'altro come "radicalmente diverso", in un processo che, attraverso una svalutazione sistemica dei gruppi di appartenenza differenti dal proprio, da un'iniziale de-legittimazione può giungere a una vera e propria de-umanizzazione[4], spesso prodromica a veri e propri crimini d'odio[5].

A fronte di conseguenze potenzialmente nefaste per la collettività e per l'individuo, soprattutto nel contesto di una società democratica e pluralista nella quale la diversità rappresenta un valore da tutelare e non un motivo di discriminazione, è noto come in più occasioni sia stato

[1] Pur a fronte di numerosi testi normativi che vi si riferiscono più o meno direttamente, un tentativo di dare una definizione istituzionale dell'"*hate speech*" può rinvenirsi soltanto nella raccomandazione del Comitato dei Ministri del Consiglio d'Europa del 30 ottobre 1997, secondo la quale «*the term "hate speech" shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, antisemitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin*».

[2] Così, Pino (2008), p. 287 ss. Alle forme di discriminazione citate dall'Autore, deve affiancarsi quella – storicamente piuttosto diffusa – avente ad oggetto l'orientamento sessuale, rispetto alla quale sono noti i tentativi – allo stato non andati a buon fine – di predisporre, anche nell'ordinamento italiano, strumenti legislativi di carattere penale finalizzati al suo contrasto. Sul tema, tra i numerosi contributi, Dolcini (2014), p. 7 ss.; Id. (2011), p. 1393 ss.; Pelissero (2015), p. 14 ss.; Goisis (2015), p. 40 ss.; Id. (2012); Pugiotto (2015), p. 6 ss.; Id. (2013), p. 71 ss.; Riccardi (2013), p. 84 ss.; Pane (2015).

[3] In questo senso, Pino (2008), p. 293-294; analogamente, Spena (2017), p. 577, il quale, tuttavia, evidenzia come, nel contrasto ai discorsi d'odio, la società finisca per usare – seppure nell'ottica di proteggerne i destinatari – le stesse categorie concettuali stereotipanti: « se il discorso d'odio fa del proprio destinatario non una persona ma l'istanza di una categoria stereotipata, la stigmatizzazione sociale, come anche la criminalizzazione, del discorso d'odio fanno altrettanto, poiché proteggono la "vittima" non per il suo essere individuo, ma in quanto istanza di quella stessa categoria stereotipata».

[4] Così, Pugiotto (2013), p. 72; nonché, Spena (2017), p. 603, secondo cui l'universo concettuale dell'odiatore «non conosce individui, ma solo categorie, gruppi, masse, tipi di soggetti; il suo contenuto di pensiero non ha mai a che fare con persone considerate per le loro caratteristiche uniche e irripetibili; anche quando si rivolga immediatamente contro un individuo, questi ne costituisce sempre e soltanto l'oggetto occasionale: l'individuo non vi è considerato *in quanto tale*, ma solo in quanto preteso esponente di una categoria. Il discorso d'odio, di conseguenza, è anche un *discorso-sineddoche*: identifica il tutto con la parte ed attribuisce a questa un valore totalizzante».

[5] In questo senso, per tutti, A. Pugiotto (2013), p. 73. Non manca, tuttavia, chi ritiene che, ove l'*hate speech* sia in grado di provocare atti di violenza non sarebbe realmente un "discorso" ma, piuttosto, un'azione: così Troper (1997), p. 189 ss. In questa prospettiva, meritano una menzione anche le note tesi sviluppatesi in Nord America nell'ambito della *Critical Race Theory*, secondo cui il discorso d'odio è idoneo a determinare danni non solo ove sfoci in atti di aggressione fisica, ma anche in quanto tale. Più specificamente, secondo i teorici della CRT, i discorsi d'odio produrrebbero un eterogeneo campionario di conseguenze negative su scala sia "individuale", identificabili in pregiudizi di tipo psichico (quali ansia, depressione, perdita di autostima, panico) o alla vita di relazione (limitazioni della propria sfera di autonomia personale per il timore di subire aggressioni o umiliazioni), che "sociale". Queste ultime, in particolare, vengono individuate anzitutto nel c.d. *silencing effect*, definito come l'effetto di privare gli appartenenti ad un determinato gruppo del proprio diritto ad essere ammessi come *partner* paritari e affidabili agli scambi comunicativi che si svolgono nella scena pubblica, sul duplice terreno delle relazioni sociali e delle rivendicazioni politiche, quale conseguenza della loro esposizione ad un clima di costante aggressione, umiliazione, denigrazione; secondariamente, si rileva come un'alta concentrazione di messaggi ostili alla parità tra individui nell'ambiente avrebbe l'effetto di legittimare e riconfermare le condizioni materiali di subalternità sociale, squilibrio economico e subordinazione gerarchica in cui versano le minoranze svantaggiate nei confronti dei gruppi sociali dominanti. Per una sintesi ricostruttiva delle posizioni del movimento, nella letteratura italiana, anche criticamente, cfr., Pino (2008), p. 297 ss.; Manetti (2005), p. 103 ss.; Visconti (2008), p. 161 ss.; Tesauro (2013), p. 67 ss.

sollecitato l'intervento del legislatore penale[6] – soprattutto da fonti e istituzioni internazionali e sovranazionali, dimostratesi particolarmente sensibili all'obiettivo di garantire l'uguaglianza tra i cittadini e la libertà da qualsiasi forma di discriminazione[7].

Non è possibile in questa sede affrontare le numerose problematiche sollevate dalla criminalizzazione dei discorsi d'odio.

Basti osservare come l'esigenza di colpire le manifestazioni di intolleranza nei confronti di un singolo o di un gruppo di individui, idonee a lederne l'uguaglianza e la dignità[8] – trattandosi di condotte di opinione, non connotate dall'uso della violenza fisica – , si ponga in conflitto con la libertà, anch'essa fondamentale, di espressione, che, in quanto condizione sostanziale per il progresso e lo sviluppo della società, è chiamata a garantire pure le affermazioni sgradevoli o ripugnanti[9].

D'altra parte, anche a voler ritenere che i discorsi d'odio – poiché in grado di negare il va-

[6] Nell'ordinamento italiano, le istanze di criminalizzazione dei discorsi d'odio si sono notoriamente tradotte nell'introduzione – ad opera dell'art. 3 della già citata L. 13 ottobre 1975, n. 654 – dei reati di diffusione di idee razziste (primo comma, lett.a)), di incitamento alla discriminazione e alla violenza razzista (primo comma, lett. b)) e di associazione finalizzata ad incitare all'odio o alla discriminazione (secondo e terzo comma). Tali disposizioni sono state oggetto di successive modifiche, prima con l'entrata in vigore del D.L. n. 122 del 1993, convertito con modifiche dalla L. 25 giugno 1993, n. 205 (c.d. Legge Mancino), che ha riformulato le norme previgenti ed introdotto la circostanza aggravante, avente portata generale, della finalità di discriminazione o di odio; poi, con la L. 24 febbraio del 2006, n. 85, che ha ulteriormente novellato i termini definitori delle condotte penalmente rilevanti, sostituendo i verbi "diffondere" e "incitare", rispettivamente, con "propagandare" e "istigare". Per una panoramica di tale quadro normativo, *ex plurimis*, Riondato (2006); De Francesco (1994), p. 174 ss.; Fornari (2007), p. 1034 ss.; Fronza (1997), p. 32 ss.; Moccia (1997), p. 90 ss.; Stortoni (1994), p. 14 ss.; Padovani (2006), p. 23 ss.; Pelissero (2006), p. 959 ss.; Pavich – Bonimi (2014); Picotti (2006), p. 1966 ss.; Visconti (2006), p. 223 ss.; Id. (2008), p. 191 ss. Nella manualistica, M. La Rosa (2014), p. 369 ss.
Più di recente, il legislatore ha introdotto, con la L. 16 giugno 2016, n. 115, l'aggravante di negazionismo (ulteriormente modificata dalla L. 20 novembre 2016, n. 167), in forza della quale si applica «la pena della reclusione da due a sei anni se la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale, ratificato ai sensi della legge 12 luglio 1999, n. 232». Sulla neo-introdotta aggravante e, più in generale, sulla criminalizzazione del negazionismo, si veda, anche in senso critico, Di Giovine (2006), p. XIII; Fronza (2012); Id. (2017), p. 155 ss.; Cassano (2014), p. 279 ss.; Caputo (2014), p. 63 ss.; Pulitanò (2015); Cavaliere (2016), p. 999 ss.; Brunelli (2016), p. 978 ss.; Puglisi (2016); De Flammineis (2016; Scotto Rosato (2016), p. 280 ss.
Da ultimo, le disposizioni fin qui citate sono state trasferite all'interno del codice penale ed inserite al Capo III del Titolo XII del Libro II c.p., che disciplina i "Delitti contro l'eguaglianza": sul punto, per tutti, Puglisi (2018), p. 1325 ss.

[7] Volendo soffermarsi esclusivamente sulle iniziative a carattere normativo, in ambito internazionale deve menzionarsi la Convenzione ONU "sull'eliminazione di tutte le forme di discriminazione razziale" adottata il 21 dicembre del 1965, e ratificata dall'Italia con la L. 13 ottobre 1975, n. 654, la quale impone agli stati membri di introdurre leggi che vietino i discorsi che incitano all'odio e che criminalizzino l'appartenenza a organizzazioni razziste; nonché il Patto internazionale per i diritti civili e politici, concluso a New York nel 1966, il quale all'art. 20.2 chiede che sia vietato per legge «qualsiasi appello all'odio nazionale, razziale o religioso che costituisca incitamento alla discriminazione, all'ostilità o alla violenza». Volgendo lo sguardo alla sfera di competenza del Consiglio d'Europa, devono ricordarsi la già citata Raccomandazione del Comitato dei Ministri del 30 ottobre 1997, a cui si affianca il Protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica, firmato a Strasburgo il 28 gennaio 2003, relativo all'incriminazione dei comportamenti di natura razzista e xenofoba diffusi tramite l'utilizzo di sistemi informatici, oltre al generale divieto di discriminazione sancito all'art. 14 della CEDU. Da ultimo, nel più ristretto quadro dell'Unione europea, deve segnalarsi – accanto al divieto di discriminazione sancito all'art. 21 della CDFUE –, la direttiva 2000/43/CE del Consiglio, del 29 giugno 2000, che attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica; ma soprattutto, la Decisione quadro 2008/913/GAI, del 28 novembre 2008, sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale, che impegna gli Stati membri a rendere punibili i comportamenti di stampo razzista e xenofobo, quali, in particolare, «l'istigazione pubblica alla violenza o all'odio nei confronti di un gruppo di persone, o di un suo membro, definito in riferimento alla razza, al colore, alla religione, all'ascendenza o all'origine nazionale o etnica», nonché «l'apologia, la negazione o la minimizzazione grossolana dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra», quando però tali comportamenti siano posti in essere in modo atto a istigare alla violenza o all'odio nei confronti di gruppo – o di un suo membro – «definito in riferimento alla razza, al colore, alla religione, all'ascendenza o all'origine nazionale o etnica».

[8] È noto come, a fronte di un'impostazione originaria della L. n. 654 del 1975 che dava rilievo primario alla tutela dell'ordine pubblico, con l'entrata in vigore della Legge Mancino, la dottrina prevalente ha individuato, quali oggettività giuridiche tutelate dalla legge, la dignità umana e l'uguaglianza: sul punto, per tutti, De Francesco (1994), p. 179. Tale impostazione ha trovato conferma anche nella giurisprudenza, a partire dalla celebre vicenda processuale che ha visto protagonisti alcuni dirigenti veronesi della Lega Nord, rinviati a giudizio per avere raccolto firme (in vista di una petizione popolare) e diffuso manifesti con i quali si sollecitava l'amministrazione cittadina ad espellere i rom e a smantellare i loro insediamenti irregolari dal territorio scaligero: cfr., anche per i richiami giurisprudenziali, Visconti (2008), p. 141 ss.
Non può, tuttavia, tralasciarsi di evidenziare come non manchi chi ritiene che tali beni, almeno per il modo in cui vengono comunemente intesi, rischiano di venire in rilievo in una dimensione astratta e collettiva, caratterizzata da una scarsa afferrabilità materiale, tale da rendere evanescente e incorporea l'offesa che potrebbe essergli arrecata da singole condotte aggressive. Sul tema, più ampiamente, Tesauro (2013); Id. (2016), p. 961 ss.

[9] In questo senso si è espressa, sin dagli anni '60, la Corte Costituzionale, evidenziando la necessità di assicurare alla libertà di espressione il più ampio riconoscimento, in quanto "pietra angolare" della democrazia: cfr., Corte Cost., sent. n. 11 del 1968, in www.giurcost.org; Corte Cost., sent. n. 168 del 1971, *ivi*; Corte Cost., sent. n. 9 del 1965, *ivi*; Corte Cost. n. 84 del 1969, *ivi*; Corte Cost., sent. n. 126 del 1985, *ivi*. Le stesse conclusioni emergono guardando alla giurisprudenza della Corte di Strasburgo, la quale ricomprende all'interno della garanzia sancita dall'art. 10 Cedu anche quelle espressioni che non offrono un significativo contributo allo sviluppo democratico e alla formazione dell'opinione pubblica, e che presentano un contenuto raccapricciante e disturbante: così, Corte edu, Gran Camera, 7 dicembre 1976, *Handysude c. Regno Unito*; Corte edu, 10 luglio 2003, *Murphy c. Irlanda*; Corte edu, 28 marzo 2008, *Azevedo c. Portogallo*.

lore stesso della persona, così come garantito agli artt. 2 e 3 Cost. – non rientrino nell'ambito di tutela della libertà di manifestazione del pensiero, la quale non può spingersi sino a negare i principi fondamentali e inviolabili del nostro ordinamento[10], appare tutt'altro che pacifica la legittimità del ricorso allo strumento penale, non potendosi ritenere per nulla scontato che questo risulti il più efficace per assicurare il contenimento delle condotte offensive[11].

La questione, già problematica, della rilevanza penale degli *hate speech* trova oggi nuovi profili di criticità ove si guardi al ruolo attualmente svolto dalle tecnologie informatiche.

Certamente le espressioni d'odio non sono un fenomeno legato allo sviluppo tecnologico, avendo trovato spazio anche in passato, verbalmente o mediante i *media* tradizionali: odiare, insomma, si è sempre odiato[12]; volgendo, però, lo sguardo ai contemporanei strumenti di comunicazione digitali, non passa inosservato come l'affermazione di internet e, soprattutto, dei *social network* abbia determinato un'accentuazione – quantomeno dal punto di vista quantitativo – delle forme di intolleranza[13].

A voler indagare – seppure brevemente – sulle ragioni alla base di siffatto incremento dell'odio, deve rilevarsi come, pur in assenza di differenze contenutistiche tra l'*online* e l'*offline hate speech*, alcune componenti strutturali della rete fungano da fattori agevolatori dei messaggi discriminatori, aumentandone di conseguenza le potenzialità lesive[14].

Più specificamente, tali componenti possono essere individuate nella velocità istantanea di diffusione dei messaggi; nella possibilità di raggiungere immediatamente milioni di destinatari; nella capacità del contenuto offensivo di sopravvivere per un lungo arco di tempo oltre la sua immissione, anche in parti del *web* diverse da quelle della sede in cui era stato originariamente inserito; e, infine, nella natura transnazionale degli intermediari informatici, che solleva evidentemente la necessità di una cooperazione tra gli Stati e le loro diverse giurisdizioni[15].

A ciò si aggiunga – da un punto di vista più sociologico – che la comunicazione al tempo dei *social* ha radicalmente ridefinito le coordinate del discorso pubblico: all'interno delle piattaforme digitali, chiunque può esternare il proprio pensiero, senza che sia necessario appartenere a una specifica categoria "elitaria", alimentando una miriade di conversazioni, che, con "un *like*", "un *retweet*", "una condivisione", si diffondono nello spazio cibernetico e raggiungono milioni di utenti in tutto il mondo. Sono mutati, in sostanza, i meccanismi tipici della comunicazione di massa: il pubblico non ha più il ruolo esclusivo di destinatario del messaggio, ma è lui stesso protagonista attivo nella divulgazione delle proprie parole verso una piazza sconfinata di persone[16].

E, tuttavia, a questa espansione delle occasioni per parlare pubblicamente non si accompagna sempre un corrispondente rafforzamento delle inibizioni a farlo. Più specificamente, la possibilità di operare in anonimato, da un lato, e «il conflitto cognitivo-percettivo tra la privatezza della situazione fisica di partenza e la pubblicità potenziale del luogo virtuale di destinazione del messaggio», dall'altro, frenano lo scattare di quei meccanismi di pudicizia – psicologica o istituzionale – che, di solito, bloccano gli individui dall'esprimere tutto quello che pensano, ivi compresi i sentimenti più cattivi, generalmente non accettati nel mondo *offline*[17].

[10] In questo senso, *ex plurimis*, De Francesco (1994), p. 179; Ambrosetti (2006), *Beni giuridici tutelati e struttura delle fatti-specie: aspetti problematici nella normativa penale contro la discriminazione razziale*, in *Discriminazione razziale,* cit., p. 93 ss.; Picotti (2006), p. 117 ss.; Salotto (2006), p. 167 ss.

[11] In questa prospettiva, Salotto (2006), p. 176 ss, secondo cui la scelta di incriminare i discorsi d'odio non si pone in contrasto con la libertà di espressione, ma, piuttosto, con il principio penalistico di sussidiarietà, sussistendo per tali fattispecie il rischio che la pena assuma carattere simbolico ed esprima valutazioni etico-sociali. In senso parzialmente critico rispetto al ricorso alla sanzione penale, più di recente, Puglisi (2018), p. 1352 ss., il quale sottolinea l'inefficacia, sotto il profilo rieducativo, dell'apparato sanzionatorio attualmente predisposto in materia di *hate speech*, fondato esclusivamente sulle pene "tradizionali" detentive e pecuniarie: a ben vedere, infatti, il diritto penale non potrebbe reagire al discorso d'odio con sanzioni de-socializzanti, dovendosi, piuttosto, favorire un contatto più ravvicinato del colpevole con la dimensione socio-culturale da lui avversata; in tale ottica – a parere dell'Autore – ben più appropriato risulterebbe il ricorso al lavoro di pubblica utilità, indirizzato in particolare alle comunità rappresentative dei gruppi offesi dalle condotte discriminatorie.

[12] Così, Spena (2017), p. 577.

[13] In questo senso, anche per ulteriori riferimenti bibliografici, Gasparini (2017), p. 505 ss. Di diverso avviso, Spena (2017), p. 577 ss., secondo cui il sentimento dell'odio, più che aumentato, sarebbe mediaticamente sovraesposto.

[14] Così, per tutti, Gasparini (2017), p. 507 ss.

[15] Più specificamente, un recente studio commissionato dall'UNESCO ha messo in luce come i fattori peculiari che contraddistinguono i contenuti digitali rispetto a quelli tradizionali debbano essere identificati nella *permanence*, nella *itinerancy*, nell'*anonymity* e nel *cross-jurisdictional character*: così, Gardaglione – Gal – Alvez – Martinez (2015), p. 13 ss.
Non manca, tuttavia, chi ritiene che la rete sia, in realtà, da intendersi come strumento "neutro", da valorizzare, anzi, come canale dotato di "forza positiva" per coordinare tutte quelle azioni che mirano a contenere e contrastare il fenomeno dell'odio: cfr., Ziccardi (2016).

[16] In questa prospettiva, più ampiamente, Spena (2017), p. 578 ss., che ricostruisce i meccanismi della comunicazione all'interno delle piattaforme digitali come quelli tipici dell'agire in massa.

[17] Spena (2017), p. 579 ss.

L'anonimato, peraltro, oltre a facilitare l'emersione di quelle pulsioni negative normalmente trattenute, fa cadere – o comunque attenua notevolmente – la probabilità di essere chiamati a rispondere per i propri comportamenti, diminuendo di conseguenza il senso di responsabilità e il timore della sanzione[18].

Da ultimo, quale ulteriore fattore in grado di facilitare le manifestazioni d'odio in rete, non può non considerarsi la mancanza di un contatto fisico diretto con la vittima: a ben vedere, infatti, la distanza materiale che caratterizza i sistemi *online* non solo favorisce quel processo di stereotipizzazione e, consequenziale, de-umanizzazione dell'altro, posto alla base di tutti gli *hate crimes*; ma, soprattutto, non consente all'odiatore di vedere l'esito di sofferenza delle proprie azioni, impedendogli così di identificarsi come persona cattiva che fa del male ai suoi simili[19].

A fronte degli evidenziati rischi che la comunicazione 2.0 determina rispetto alla propagazione degli *hate speech*, occorre, dunque, interrogarsi su quali siano i più efficaci strumenti di contrasto del fenomeno, ma soprattutto se, ed entro quali limiti, sia legittimo configurare eventuali responsabilità in capo agli intermediari informatici, stante il contributo che gli stessi apprestano alla diffusione e alla permanenza in rete dei contenuti digitali.

2. La strategia europea di contrasto all'odio *online*.

L'esigenza di ostacolare l'affermazione dell'odio in rete è emersa, anzitutto, nell'ambito delle Istituzioni europee, le quali, negli ultimi anni, hanno messo progressivamente in atto una strategia finalizzata a fronteggiarne la diffusione.

Si tratta, a ben vedere, di una regolamentazione che si inserisce nel solco della più generale attenzione riservata – come si è accennato – dall'Europa, e dagli altri organismi internazionali, ai temi della dignità umana e dell'uguaglianza tra i cittadini: nell'ottica europea, i fenomeni discriminatori si ripercuotono negativamente non solo sui gruppi o sui singoli presi di mira, ma anche su tutti coloro che nella società si esprimono a favore della libertà e della tolleranza – finendo per incidere così sul sistema democratico –, e richiedono, pertanto, politiche attive di contenimento[20].

In tale prospettiva – e in accordo con quanto stabilito dalla decisione quadro 2008/913/GAI del Consiglio, sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale[21] –, già con l'Agenda europea sulla sicurezza del 2015, è stato istituito, su iniziativa della Commissione, un Internet Forum, che riunisce i Ministri degli Interni degli Stati membri dell'Unione europea, nonché i rappresentanti dei principali fornitori di servizi via Internet, del Parlamento europeo, di Europol, e il coordinatore europeo per la lotta al terrorismo. Obiettivo del Forum è quello di individuare sistemi che ostacolino la diffusione di contenuti che inneggiano all'odio, alla violenza e al terrorismo internazionale[22].

In esito a siffatta iniziativa, è stata predisposta un'attività di rilevazione e monitoraggio della casistica del fenomeno, al fine di creare sempre maggiore consapevolezza nei cittadini e nelle istituzioni, a cui si è affiancata la previsione di iniziative di *counter-speech*, o contro-discorso, con l'obiettivo, da un lato, di spiegare il perché l'odio sia profondamente anti-democratico; dall'altro, di riaffermare i valori che lo stesso mette in pericolo[23].

All'approccio statistico-culturale si è accompagnata, poi, la sollecitazione delle piattaforme *web* a porre in essere meccanismi di prevenzione e rimozione dei contenuti offensivi pubblicati sui loro portali.

[18] Spena (2017), p. 582.
[19] Spena (2017), p. 583. Su tali profili, nella prospettiva più generale dei *cybercrime*, per tutti, Picotti (2000), p. 1 ss.
[20] Sul punto, cfr., da ultimo, il "*Codice di condotta per lottare contro le forme illegali di incitamento all'odio* online", consultabile su https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300.
[21] Sulla decisione quadro, cfr., Lobba (2011), p. 109 ss.; Mancuso (2009), p. 645 ss.; Moschetta (2014), p. 781 ss.
[22] Cfr., http://europa.eu/rapid/press-release_IP-15-6243_en.htm.
[23] Sotto questo profilo, si consideri, esemplificativamente, lo studio su "*The European legal framework on hate speech, blasphemy and its interaction with freedom of expression*", realizzato dal Direttorato-generale per le politiche interne presso il Parlamento europeo e consultabile su http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)536460. Alle iniziative elaborate in seno all'Unione Europea si affiancano, poi, quelle sviluppate nell'ambito del Consiglio d'Europa e, più specificamente, dalla *European Commission against Racism and Intolerance* (ECRI), il cui obiettivo è proprio quello di monitorare la situazione dei Paesi membri con riferimento a fenomeni di razzismo, intolleranza e discriminazione, emettendo – ove necessarie – specifiche raccomandazioni: https://www.coe.int/web/european-commission-against-racism-and-intolerance/ .

Sotto questo profilo, particolarmente significativo risulta l'accordo raggiunto tra la Commissione Ue e i principali intermediari di servizi internet (Microsoft, Facebook, Twitter e Youtube; successivamente, Instagram, Google+, Snapchat e Dailymotion), con cui è stato elaborato un codice di condotta finalizzato a contrastare le condotte di *hate speech*[24]. Tra i numerosi impegni assunti, si possono indicativamente citare: l'adozione di procedure chiare ed efficaci per esaminare le segnalazioni riguardanti forme illegali di incitamento all'odio nei servizi da loro offerti, in modo da poter rimuovere tali contenuti o disabilitarne l'accesso; l'adozione di linee-guida indirizzate alla comunità degli utenti della rete, che precisino il divieto di ogni forma di istigazione all'odio e alla violenza; l'obbligo di esaminare, entro 24 ore dalla ricezione, la maggior parte delle segnalazioni (valide) di illecita istigazione all'odio nei servizi offerti dal *provider* e, se necessaria, la rimozione di tali contenuti o la disabilitazione dell'accesso al sito[25].

Sennonché, pur a fronte dei progressivi miglioramenti monitorati dalla Commissione[26], le criticità ancora persistenti in ordine alla tempestività e all'effettività dei meccanismi di rimozione spingono a dubitare dell'efficacia di una strategia fondata esclusivamente sull'autoregolamentazione, indirizzando, piuttosto, verso una più incisiva e vincolante definizione delle responsabilità degli intermediari informatici, alla stregua di quanto già previsto per altri settori di disciplina, come la tutela del diritto d'autore, la pedopornografia o il terrorismo[27].

La questione, a ben vedere, si inserisce nell'ambito del più ampio dibattito che ha interessato, nell'ultimo ventennio, la dottrina e la giurisprudenza, circa la possibilità di configurare una responsabilità dell'Internet *provider* per i fatti commessi *online* attraverso il suo *server* oppure mediante gli accessi alla rete che egli concede agli utenti. Si tratta – come vedremo –

[24] Per una ricognizione delle attività che hanno portato all'elaborazione del Codice di Condotta, cfr., https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300.

[25] Cfr., *Codice di condotta per lottare contro le forme illegali di incitamento all'odio* online, cit.

[26] I risultati del primo monitoraggio sull'efficacia del Codice di condotta – realizzato da 12 organismi indipendenti con sede in vari Stati membri dell'Unione – hanno evidenziato come, a fronte di oltre 600 segnalazioni, solo nel 28,2% dei casi il contenuto illecito è stato rimosso: https://ec.europa.eu/newsroom/just/item-detail.cfm?&item_id=50840. Un incremento delle rimozioni a seguito di segnalazioni degli utenti, fino al 59% dei casi in media è stato riscontrato in esito alla seconda valutazione, i cui risultati sono stati pubblicati nel giugno 2017; è, tuttavia, emerso come soltanto alcune delle piattaforme digitali abbiano sviluppato un sistema di procedure tempestive e chiare agli utenti, per la segnalazione e rimozione dei messaggi illeciti: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=71674. Un quadro analogo è risultato anche dal terzo monitoraggio, rilasciato nel gennaio del 2018: a fronte di un ulteriore aumento dei casi di rimozione, pari a circa il 70 % delle segnalazioni, continuano a permanere significative differenze nei sistemi di rimozione tra le singole società digitali: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=612086. In considerazione di questi risultati non ancora del tutto soddisfacenti, il 1° marzo 2018, la Commissione ha adottato una Raccomandazione (C(2018) 1177 final), contenente una serie di misure operative, indirizzate sia alle aziende che operano in rete, sia agli Stati membri, "*to effectively tackle illegal content online*": https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online.

[27] In materia di tutela del diritto d'autore viene in rilievo la disposizione contenuta nel D.L. 22 marzo 2004, n. 72, convertito con L. 21 maggio 2004, n. 128, recante *Interventi per contrastare la diffusione telematica abusiva di opere dell'ingegno, nonché a sostegno delle attività cinematografiche e dello spettacolo*, che all'art. 1, commi 6 e 7, stabilisce l'obbligo per i *provider* – a seguito di provvedimento dell'autorità giudiziaria – di porre in essere tutte le misure dirette ad impedire l'accesso ai contenuti dei siti o a rimuoverli, pena l'applicazione di una sanzione amministrativa pecuniaria da euro 50.000 a euro 250.000. A ciò si aggiunga quanto previsto dall'art. 163 della L. 22 aprile 1941, n. 633, come modificato da D.Lgs. 16 marzo 2006, n. 140, di attuazione della direttiva 2004/48/CE sul rispetto dei diritti di proprietà intellettuale, che al comma 1 stabilisce che «Il titolare di un diritto di utilizzazione economica può chiedere che sia disposta l'inibitoria di qualsiasi attività, ivi comprese quelle costituenti servizi prestati da intermediari, che costituisca violazione del diritto stesso...». Su tale disciplina, più ampiamente, FLOR (2010).
Per ciò che concerne la pedopornografia, il riferimento è alla disciplina dettata dall'art. 14 quater della L. 3 agosto 1998, n. 269, introdotto dalla L. 6 febbraio 2006, n. 38, il quale stabilisce l'obbligo per i fornitori di connettività alla rete internet di utilizzare strumenti di filtraggio e le relative soluzioni tecnologiche conformi ai requisiti individuati con decreto dal Ministro delle comunicazioni, di concerto con il Ministro dell'innovazione e le tecnologie, per impedire l'accesso ai siti segnalati dal Centro nazionale per il contrasto alla pedo-pornografia sulla rete Internet, istituito presso il Ministero dell'Interno, pena l'applicazione di una sanzione amministrativa pecuniaria compresa tra i 50.000 e i 250.000 euro. Su tale disciplina, più ampiamente, Picotti (2007), p. 1207 ss. Si tratta, a ben vedere, di una disposizione in linea con quanto previsto dall'art. 25 della successiva Direttiva 2011/93/UE in materia di lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, a norma del quale «gli Stati membri possono adottare misure per bloccare l'accesso alle pagine web che contengono o diffondono materiale pedopornografico agli utenti internet sul loro territorio», purché siano stabilite con procedure trasparenti, che forniscano idonee garanzie per assicurare che la restrizione sia limitata, necessaria e proporzionata e che gli utenti siano informati del motivo della restrizione: cfr., https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32011L0093&from=IT.
Con riferimento, invece, al terrorismo, deve segnalarsi la previsione dell'art. 2, comma 3, del D.L. 18 febbraio 2015, n. 7, convertito con la L. 17 aprile 2015, n. 43, contenente misure urgenti per il contrasto al terrorismo anche di matrice internazionali, a norma della quale i fornitori di connettività, su richiesta dell'autorità giudiziaria procedente, devono inibire l'accesso ai siti utilizzati per le attività e le condotte aventi finalità di terrorismo, secondo le modalità, i tempi e le soluzioni tecniche individuate e definite con il decreto previsto dall'articolo 14-quater, comma 1, della legge 3 agosto 1998, n. 269. Su tale normativa, più ampiamente, Signorato (2015), p. 55 ss. Non può tralasciarsi, peraltro, come la Commissione UE abbia recentemente annunciato la predisposizione di un regolamento finalizzato proprio al contrasto dei contenuti terroristici sul *web*, in forza del quale sarà imposta ai prestatori di servizi informatici operanti nel territorio dell'Unione l'istituzione di specifici meccanismi di reclamo che consentano la rimozione dei contenuti illeciti, entro un'ora dall'ordine emesso dalle autorità, pena l'applicazione di sanzioni pecuniarie il cui ammontare potrà raggiungere anche il 4% del loro fatturato complessivo: cfr., http://europa.eu/rapid/press-release_IP-18-5561_it.htm.

di una tema alquanto complesso, che costringe a fare i conti con le problematiche tipiche delle forme di manifestazione del reato, rese ancora più articolate dalle peculiari caratteristiche che l'*Internet service provider* presenta, in quanto soggetto non fisico che opera in un non luogo[28].

3. I paradigmi di responsabilizzazione dell'*Internet Service Provider* nel formante legislativo, dottrinale e giurisprudenziale.

Volendo tratteggiare – sia pure sinteticamente – le questioni dogmatiche e applicative che il tema della responsabilizzazione dell'Isp pone, va evidenziato come ogni discussione in ordine a siffatti profili non possa che muovere da una valutazione inerente al ruolo sociale da attribuire al *provider*, potendosi immaginare – riprendendo una schematizzazione proposta in dottrina[29] – tre distinti paradigmi idealtipici.

1) Il primo modello di responsabilità si caratterizza per la massimizzazione della libertà di comunicazione e di espressione: l'Isp è posto sullo stesso piano degli altri utenti e, pertanto, è privo di doveri di controllo rispetto alle condotte altrui, di obblighi di denuncia o di oneri di collaborazione con l'autorità; il ruolo sociale riconosciutogli è quello del comune cittadino e, di conseguenza, sul piano penalistico, la sua responsabilità è limitata alle ipotesi di autoria o di concorso commissivo doloso nell'altrui condotta criminosa.

2) Il secondo paradigma si contraddistingue, invece, per assicurare la più ampia tutela dei soggetti terzi e della comunità, seppure a fronte di significative limitazioni della libertà di comunicazione degli utenti: secondo tale modello, l'Isp è tenuto a una attività di controllo e di censura preventiva del materiale caricato, assumendo il ruolo sociale di controllore. Dal punto di vista penalistico, lo schema di responsabilità è quello del reato omissivo improprio e, in particolare, il rimprovero è quello di non aver impedito il reato altrui.

3) Il terzo modello di responsabilità si pone in una posizione intermedia tra i primi due: l'attività di repressione dei reati commessi in rete coinvolge l'Isp solo *ex post*, imponendogli l'obbligo di denuncia degli illeciti di cui viene a conoscenza, oneri di collaborazione con le autorità nell'individuazione degli autori degli illeciti e obblighi di rimozione del materiale illecito. Il ruolo sociale dell'Isp è quello di tutore dell'ordine e il paradigma di responsabilità, dal punto di vista penalistico, è quello del reato omissivo proprio.

Tutto ciò premesso, due aspetti possono ritenersi sin da ora pacifici: il primo riguarda la possibilità che il *provider* sia chiamato a rispondere per i reati commessi attraverso le sue strutture se, oltre a fornire gli accessi alla rete, è autore, o co-autore, dei contenuti o dell'attività di diffusione illecita[30].

Il secondo, ancor più significativo, attiene al rifiuto di ogni forma di controllo preventivo e generale sulle attività svolte dagli utenti, trattandosi di un intervento "inesigibile"[31] per ragioni economiche – in quanto eccessivamente oneroso –; pratiche – in considerazione della struttura "aperta" che caratterizza Internet –; ma soprattutto giuridiche, non ricorrendo – a ben vedere – nessuna delle condizioni necessarie a configurare una responsabilità per omesso impedimento del reato altrui, *ex* art. 40 cpv c.p.[32].

Invero, anche prescindendo dal fatto che è a tutt'oggi controversa la possibilità di riferire la citata clausola di equivalenza a delitti non causalmente orientati, che tutelino beni diversi dalla

[28] Così, per tutti, Ingrassia (2012), p. 15 ss.
[29] Ingrassia (2012), p. 5 ss.
[30] In questo senso, *ex plurimis*, Seminara (1997), p. 96 ss.; Ruggiero (2001), p. 586 ss.; Petrini (2004), p. 130 ss; Spagnoletti (2004), p. 1922 ss.; Flor (2010), p. 444; Ingrassia (2012), p. 7 ss.; Bartoli (2013), p. 604. Non manca, peraltro, chi ritiene necessario distinguere a seconda che il fatto commesso dall'Isp rientri nella categoria dei reati cibernetici in senso stretto, ovvero illeciti che già prevedono nel tipo una connessione con la rete, o in quella dei reati cibernetici in senso lato, cioè fattispecie tradizionali che per la descrizione elastica della situazione tipica consentono una loro realizzazione anche in internet. Se rispetto ai primi non si porrebbero dubbi sulla possibilità di autoria del *provider*, più complessa sarebbe la possibilità di realizzazione monosoggettiva dei secondi, dovendosi guardare, di volta in volta, alla specifica descrizione del fatto tipico: per tale prospettiva, cfr., Petrini (2004), p. 120 ss.; Ingrassia (2012), p. 8 ss.
Per ciò che concerne, invece, le ipotesi di partecipazione concorsuale o coautoria – a fronte di una dottrina e una giurisprudenza maggioritarie che ne riconoscono la piena configurabilità – , deve segnalarsi la posizione di chi ritiene che il concorso commissivo dell'Isp potrebbe essere integrato solo in casi limitati, assistiti da un dolo di partecipazione particolarmente intenso e da un'oggettiva possibilità di impedire la commissione del reato: così, Seminara (1997), p. 101; Petrini (2004), p. 147 ss.; Flor (2010), p. 463-464.
[31] La categoria dell'esigibilità è richiamata da Fornasari (2004), p. 423 ss.
[32] In questo senso, *ex plurimis*, Seminara (1998), p. 745 ss.; Manna (2001), p. 145 ss.; Ruggiero (2001), p. 586 ss.; Corrias Lucente (2004), p. 2523 ss.; Petrini (2004), p. 178; Spagnoletti (2004), p. 1922 ss.; Ingrassia (2012), p. 25 ss.; Bartoli (2013), p. 602; E. La Rosa (2016), p. 737-738; Panattoni (2018), p. 249-250.

vita e dall'integrità fisica[33], manca attualmente nel nostro ordinamento una norma che fondi un generale obbligo per il *provider* di impedimento dei reati degli utenti. Anzi, lo stesso legislatore, all'art. 17 del D. Lgs. n. 70 del 2003, a sua volta attuativo della direttiva europea dell'8 giugno 2000 (2000/31/CE) sul commercio elettronico, ha espressamente escluso l'esistenza di un obbligo generale di sorveglianza da parte dell'Isp sui contenuti caricati dagli utenti, nonché l'onere per lo stesso di ricercare fatti o circostanze sintomatici di attività illecite[34].

A ciò si aggiunga che non sarebbe individuabile in capo al *provider* una posizione originaria di protezione o di controllo, rispetto ai rischi e alle fonti di pericolo che non rientrano nella sua sfera di signoria: non sembra, infatti, potersi riscontrare, né una relazione sostanziale con l'utente, né beni giuridici particolarmente vulnerabili, tali da giustificare un così forte ruolo di garanzia[35]. Tantomeno, al *provider* sarebbero riconducibili, sia sul piano fattuale che su quello giuridico, particolari poteri impeditivi che gli consentano di interferire o di inibire la condotta dell'autore del reato[36].

Sennonché, pur a fronte dell'assenza di un obbligo generale di sorveglianza, non è mancato chi ha prospettato la possibilità di configurare ugualmente una responsabilità omissiva, sia in forma autonoma ex art. 40 cpv c.p., sia a titolo concorsuale, ex art. 110 c.p., per contributo omissivo di partecipazione, alla luce di specifiche disposizioni che prevedono puntuali doveri in capo all'Isp.

Potendo in questa sede soffermarci solo sulla disciplina generale dettata in materia, ossia il già citato D.Lgs. n. 70 del 2003 sul commercio elettronico, deve osservarsi come l'esclusione della possibilità di muovere al *provider* un rimprovero – anche sul piano civilistico – per i contenuti trasmessi o memorizzati, sia subordinata al rispetto di alcune condizioni individuate, rispettivamente, agli artt. 14, 15, 16, e distinte in relazione al tipo di attività svolta: *mere conduit*; *caching*; *hosting*.

Più specificamente, e in estrema sintesi, si prevede l'impossibilità di invocare l'esenzione di responsabilità stabilita in via generale dalla legge, ove il *provider*:

- in caso svolga funzioni di *mere conduit* (accesso e trasmissione di dati), non si sia limitato a tenere un ruolo passivo ed automatico nella diffusione dei *file* nella rete, o perché li abbia selezionati o perché ne abbia conosciuto il contenuto;

- in caso svolga funzioni di *caching* (memorizzazione automatica e temporanea di dati), non abbia agito prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena sia venuto effettivamente a conoscenza del fatto che le informazioni siano state rimosse o che l'accesso alle stesse sia stato disabilitato;

[33] Per tale prospettiva, per tutti, Fiandaca – Musco (2014), p. 626 ss.

[34] Tantomeno un rimprovero all'Isp può fondarsi sugli artt. 57 e 57 bis c.p., i quali – come è noto – disciplinano la responsabilità del direttore e del vice-direttore (per la stampa periodica) e dell'editore o dello stampatore (per quella non periodica) per i reati commessi col mezzo della stampa e non impediti a causa di un insufficiente controllo: a ben vedere, infatti, l'applicazione di tali norme al *provider* si risolverebbe in un'estensione analogica *in malam partem*, stante, per un verso, le sostanziali differenze che caratterizzano i due mezzi di comunicazione; per l'altro, l'impossibilità per i *provider* di verificare i contenuti pubblicati, che – a ben vedere – costituisce la ragione della responsabilità dei direttori di stampa periodica. Cfr., Zeno Zencovich (1998), p. 16; Id. (2001), p. 153 ss.; Seminara (1998), p. 750 ss.; Costanzo (2000), p. 657 ss.; Manna (2001), p. 148; De Natale (2009), p. 539 ss.; Flor (2010), p. 454; Ingrassia (2012), p. 27; Bartoli (2013), p. 603 ss.
Nello stesso senso, si esprime la prevalente giurisprudenza di merito e di legittimità, che, in diverse occasioni – pur riconoscendo la necessità di un'interpretazione evolutiva e costituzionalmente orientata del termine stampa – ha escluso la possibilità di equiparare i mezzi telematici alla stampa tradizionale, a meno che non si tratti di testate strutturate come veri e propri giornali e, dunque, dotate di un'organizzazione redazionale e di un direttore responsabile: in questo senso, da ultimo, Cass. pen., sez. V, 14 novembre 2016, n. 4873, Manduca, in www.penalecontemporaneo.it (20 aprile 2017), con nota di Birritteri (2017); nonché, con specifico riferimento alla sequestrabilità delle testate giornalistiche *online*, Cass. pen., Sez. Un., 29 gennaio 2015, n. 31022, Sallusti e altri, in www.penalecontemporaneo.it (20 luglio 2015), con nota di Melzi d'Eril (2016); in *Cass. pen.*, 2015, p. 3454 ss., con nota di Paoloni (2015); in *Giur. cost.*, 2015, p. 1055 ss., con nota di Diotallevi (2015); in *Dir. info.*, 2015, p. 1041 ss., con nota di Corrias Lucente (2015). Per una ricostruzione del dibattito, per tutti, Gullo (2015), p. 143 ss.
Non può, peraltro, tralasciarsi di segnalare che, più di recente, i giudici di legittimità hanno affermato – con un vero e proprio *revirement* – la possibilità di estendere alle testate telematiche registrate non solo le garanzie costituzionali in tema di sequestro, ma altresì lo "statuto penale" previsto per la carta stampata, sicché, anche il direttore della testata *online* può essere chiamato a rispondere ai sensi dell'art. 57 c.p.: così, Cass. pen., sez. V, 11 dicembre 2017, n. 13398, D.N., in *Guid. dir.*, 2018, 17, p. 83 ss.; Cass. pen., sez. V, 23 ottobre 2018, n. 1275, Sgroi e altri, in www.penalecontemporaneo.it (28 febbraio 2019), con nota di Mauri (2019).

[35] Così, Flor (2010), p. 454; nonché, Bartoli (2013), p. 603. A ben vedere, secondo quest'ultimo Autore, se si assume come punto di riferimento una posizione di garanzia assimilabile a quelle di controllo (vigilare e contenere la potenziale pericolosità di soggetti le cui caratteristiche personali determinano il fondato motivo di condotte pericolose), l'utente non avrebbe le peculiarità personali in grado di renderlo di per sé pericoloso; tantomeno, l'Isp avrebbe alcun legame sostanziale con l'utente. Se, invece, si assume come punto di riferimento una posizione di garanzia assimilabile a quelle di protezione (necessità di far fronte alla particolare vulnerabilità di determinati beni), non sembra potersi configurare un bene giuridico meta individuale corrispondente ad una "rete sana", rispetto al quale l'Isp rivesta il ruolo di garante da ogni fonte di pericolo.

[36] In questo senso, *ex plurimis*, Spagnoletti (2004), p. 1935-1936; Flor (2010), p. 455; Bartoli (2013), p. 603; Ingrassia (2012), p. 27.

- in caso svolga funzioni di *hosting* (memorizzazione duratura di dati) –effettivamente a conoscenza del fatto che l'attività o l'informazione realizzata sui propri *service* è illecita – non agisca immediatamente per rimuoverla (sul piano civilistico è, invece, sufficiente la cognizione di fatti o di circostanze che rendano manifesta l'illiceità dell'attività o dell'informazione).

Ora, a parere di autorevole, seppure minoritaria, dottrina, dalle disposizioni citate sarebbe ricavabile per il *provider* un vero e proprio obbligo giuridico di impedimento della protrazione dell'illecito: a ben vedere, infatti, a seguito della presenza/permanenza del reato nella rete – ancor più ove accompagnata da una comunicazione qualificata da parte delle Autorità – si verrebbe a creare quella relazione sostanziale tra l'Isp e il reato che contraddistingue le posizioni di garanzia, a cui si affiancherebbero effettivi poteri fattuali e giuridici per impedire la prosecuzione delle violazioni[37].

Si tratta, invero, di una soluzione ultimamente condivisa anche dalla giurisprudenza. Quest'ultima, in realtà, per lungo tempo si era attestata sulle stesse posizioni della dottrina maggioritaria, anche in considerazione del vigente dettato normativo che – come si è detto – respinge l'esistenza di un obbligo generale di sorveglianza in capo all'Isp.

Più specificamente, nel *leading case* in materia, noto come *Google vs. Vividown*, era stata esclusa, in tutti i gradi di giudizio, la sussistenza in capo ai *manager* della società di intermediazione informatica di un obbligo giuridico di impedire il delitto di diffamazione, perpetrato dagli utenti del sito mediante la pubblicazione di alcuni filmati sulla piattaforma *Google Video*, proprio sulla scorta dell'interpretazione della già citata normativa sul commercio elettronico[38], peraltro avallata anche da alcune decisioni della Corte di Giustizia UE[39].

Più di recente, tuttavia, si è andato affermando – soprattutto nella giurisprudenza civile di merito[40], ma altresì in una recente decisione della Cassazione[41] – un opposto indirizzo interpretativo, il quale – al contrario – riconosce la possibilità di configurare una responsabilità penale dell'*hosting provider*, a titolo di concorso omissivo nel reato commesso dall'utente, proprio in forza dell'obbligo di rimozione del materiale illecito, sancito all'art. 16 del D.Lgs. n. 70 del 2003.

In particolare, i giudici di legittimità – chiamati a decidere in ordine all'imputazione del gestore di un sito Internet che aveva ospitato un'affermazione offensiva nella sezione dei commenti –, hanno fatto leva sulla circostanza che il *provider* avesse consapevolmente mantenuto il contenuto sul proprio portale, pur avendo avuto conoscenza della sua natura illecita, senza adottare le iniziative necessarie per evitare che la condotta diffamatoria si protraesse.

A conclusioni analoghe è giunta altresì – seppure sotto il profilo civilistico – la Corte edu

[37] Per tale impostazione, cfr., Picotti (1999), p. 501 ss.; Id. (2007), p. 1207 ss.; Flor, (2010), p. 456 ss.

[38] Così, Cass. pen., sez. III, 17 dicembre 2013, n. 5107, in www.penalecontemporaneo.it (6 febbraio 2014), con nota di Ingrassia (2014); in *Dir. pen. proc.*, 2014, p. 277 ss., con nota di Corbetta (2014); in *Danno e resp.*, 2014, 3, p. 336 ss., con nota di Piergallini (2014); in *Giur. it.*, 2014, p. 2016 ss., con nota di Macrillò (2014). Come accennato, alle medesime conclusioni – quantomeno con riferimento al concorso nel delitto di diffamazione – era già pervenuto il Tribunale: Trib. Milano, sez. IV, 24 febbraio 2010, n. 1972, in www.penalecontemporaneo.it (21 aprile 2010); nonché la Corte di Appello: Corte App. Milano, 21 dicembre 2012, n. 8611, *ivi* (4 marzo 2013), con nota di Ingrassia (2013). Meno lineare è stato l'*iter* processuale per ciò che concerne l'altro delitto contestato agli imputati, cioè l'illecito trattamento dei dati personali della vittima (art. 167 D. Lgs. 196/2003, c.d. Codice della *Privacy*). Come è noto, infatti, nel giudizio di primo grado, il giudice ambrosiano ha ritenuto i *manager* di *Google* responsabili del reato, in considerazione del fatto che avrebbero dovuto avvisare gli utenti degli «obblighi agli stessi imposti dalla legge, del necessario rispetto degli stessi, dei rischi che si corrono non ottemperandoli»; obblighi derivanti, secondo lo stesso giudice, dall'art. 13 del D.Lgs. 196/2003, oltre che dal "buon senso". La Corte d'appello –e successivamente la Cassazione – non hanno, tuttavia, condiviso siffatta impostazione, ritenendo – diversamente dal Tribunale – che l'art. 167, letto in combinato disposto con l'art. 13, non preveda alcun obbligo di informare gli *uploader* sui doveri loro incombenti; e, più in generale, che la piattaforma video non sia titolare del trattamento dei dati contenuti nelle riprese finché gli stessi le siano sconosciuti, dovendosene assumere la responsabilità solo una volta ricevuta la comunicazione dell'Autorità che le imponga di rimuovere il contenuto o di non consentirne l'accesso.

[39] Il riferimento è, in particolare, a Corte di Giustizia UE, 24 novembre 2011, C-70/10, *Scarlet c. SABAM* e Corte di Giustizia, 16 febbraio 2012, C-360/10, *SABAM c. Netlog*, con cui i giudici europei hanno ribadito l'illegittimità di misure e strumenti che obblighino il *provider* a realizzare una sorveglianza generalizzata, attiva e preventiva sui dati immessi in rete dagli utenti. Cfr., altresì, Corte di Giustizia, 12 luglio 2011, C-324/09, *L'Oreal e altri c. eBay International*, con cui la Corte ha evidenziato che il *provider* può essere chiamato a rispondere per i contenuti illeciti memorizzati, solo se sia effettivamente a conoscenza dell'illegalità degli stessi e non agisca immediatamente per rimuovere le informazioni o disabilitare gli accessi.
Su tali profili, più ampiamente, D'Ambrosio (2012), p. 67 ss.

[40] Cfr., seppure in ottica civilistica, Trib. Napoli Nord, sez. II, 3 novembre 2016, in Giur. it., 2017, p. 629 ss., con nota di Bocchini (2017); in *Resp. civ. prev.*, 2017, p. 536 ss., con nota di Bugiolacchi (2017); in *Dir. info.*, 2017, p. 254 ss., con nota di Montanari (2017); Trib. Torino, 7 aprile 2017, n. 1928, in www.iusexplorer.it.; Corte App. Roma, 29 aprile 2017, n. 2883, *ivi*; Trib. Milano, ord. 8 maggio 2017, sez. impr., *ivi*; Trib. Roma, 15 febbraio 2019, n. 3512, in www.altalex.it.

[41] Cass. pen., sez. V, 27 dicembre 2016, n. 54946, in *Foro it.*, 2017, p. 251 ss., con nota di Di Ciommo (2016); in *Cass. pen.*, 2017, p. 2782 ss., con nota di Carbone (2017); in *Giurisprudenza penale* web, 2017, 1, con nota di Miglio (2017); in *Questione Giustizia* (9 gennaio 2017), con nota di Buffa (2017). Cfr., altresì, Ingrassia (2017), p. 1621 ss.

nel caso *Delfi c. Estonia*, deciso dalla Grande Camera della CEDU in data 16 giugno 2015[42]. Chiamati a decidere sulla legittimità della condanna al risarcimento dei danni emessa nei confronti di uno dei più importanti portali internet di *news* dell'Estonia, per i commenti incitanti all'odio e alla violenza pubblicati dagli utenti del sito, i giudici di Strasburgo hanno escluso la violazione del diritto alla libertà di espressione garantito all'art. 10 della Convenzione, riconoscendo la conformità della misura risarcitoria irrogata[43].

Volendo cogliere le ragioni di questo cambiamento di direzione, deve osservarsi come le tipologie e i modelli di attività dei *service provider* abbiano subito negli ultimi anni una significativa evoluzione: il riferimento è, in particolare, all'affermazione di quelle piattaforme *online*, gestite da *provider* che, alle tradizionali funzioni passive di memorizzazione dei dati, affiancano quelle di indicizzazione, categorizzazione e organizzazione delle informazioni fornite e caricate dagli utenti; organizzazione da cui, peraltro, traggono anche sostegno finanziario, in ragione dello sfruttamento pubblicitario connesso alla presentazione dei contenuti digitali. Si pensi, esemplificativamente, ai c.d. *User generated content* come *You Tube*, o ai *social network* come *Facebook*[44].

Sotto questo profilo, se appariva ben giustificabile – a fronte di un settore economico e tecnologico ancora *in nuce*[45] –, una limitazione di responsabilità per i *provider*, nei casi in cui l'attività del prestatore dei servizi informatici avesse carattere meramente tecnico, automatico e passivo – anzi, è lo stesso considerando 42 della Direttiva sull'*e-commerce* del 2000 a individuare questa come la ragione posta a fondamento dell'esenzione della responsabilità –, non può dirsi altrettanto nel caso in cui la funzione del provider sia quella sopra descritta, definita, significativamente, di "*hosting* attivo"[46].

Sennonché, pur potendosi comprendere le motivazioni poste alla base di tale mutamento

[42] Corte edu, Grande Camera, 16 giugno 2015, *Delfi c. Estonia*, in www.federalismi.it.

[43] Va, tuttavia, evidenziato come, a distanza di pochi anni dalla citata decisione, i giudici europei hanno operato una parziale distensione dei principi affermati – se non addirittura un ribaltamento. Più specificamente, con la decisione Corte edu, 2 maggio 2016, *MTE and Index. hu Zrt c. Ungheria*, è stata ritenuta contraria all'art. 10 della Convenzione la sentenza di condanna al risarcimento del danno, irrogata dal Tribunale nazionale ai gestori di due portali di informazione, in relazione ad alcuni commenti offensivi pubblicati dagli utenti nei confronti di sito *web* di intermediazione mobiliare accusato di aver commesso una frode in danno ai consumatori. Analogamente, la Corte di Strasburgo ha dichiarato l'irricevibilità dei ricorsi promossi da due soggetti destinatari di commenti diffamatori, che avevano visto respinta la richiesta di risarcimento del danno posta, sul piano del diritto nazionale, nei confronti dei gestori delle piattaforme *web* dove era avvenuta la pubblicazione. Segnatamente, con la pronuncia Corte edu, 9 marzo 2017, *Pihl c. Svezia*, i giudici hanno ritenuto corretto il bilanciamento raggiunto dalla Corte nazionale tra il diritto del ricorrente alla reputazione ed il diritto alla libertà di espressione dell'intermediario, in considerazione del fatto che le espressioni incriminate non contenevano forme di incitamento all'odio o alla violenza, ed erano comunque state rimosse entro 24 ore dalla segnalazione, rimanendo complessivamente in rete per soli 9 giorni. Allo stesso modo, nella sentenza Corte edu, 12 ottobre 2017, *Tamiz c. UK*, ha enfatizzato che l'equilibrio rinvenuto dal giudice nazionale tra libertà di espressione e diritto alla reputazione rientrasse nel margine di apprezzamento accordato alle autorità statali e che tale discrezionalità fosse particolarmente ampia in vista sia dell'esigenza di salvaguardare il contributo offerto da grandi intermediari informatici nel facilitare l'accesso alle informazioni; sia della circostanza che la maggior parte dei commenti offensivi erano solo espressioni volgari che il danneggiato, in forza del ruolo pubblico rivestito come politico, sarebbe stato chiamato a tollerare.
Sul tema, più ampiamente, Petruso (2018), p. 511 ss.

[44] In questo senso, *ex plurimis*, Panattoni (2018), p. 251; Montanari (2017), p. 254 ss.; Bocchini (2017), p. 636 ss. Quest'ultimo Autore, in particolare, evidenzia come in tale categoria rientri: « il *provider* che non si limita solo ad associare contenuti pubblicitari ai materiali immessi in Rete dagli utenti, ma offre agli inserzionisti un servizio che consente di visualizzare i messaggi pubblicitari, in relazione agli specifici contenuti propri dei video immessi dagli utenti, tramite l'utilizzo di parole chiave; – il *provider* che acquisisce il diritto di utilizzare i video immessi dagli utenti, di modificarli, di distribuirli, di adattarli e quindi riorganizza i materiali caricati sulla propria piattaforma; – il *provider* che predisponga un servizio, visibile come *link* sotto ogni video pubblicato in Rete, che consente al visitatore di segnalare al prestatore del servizio l'eventuale illiceità del contenuto immesso dall'utente e consente alla redazione di verificare la segnalazione stessa e di provvedere all'eventuale rimozione, definito quale servizio di "segnala abuso"; – il *provider* che fa sottoscrivere ai suoi utenti dei contratti che prevedono sia una licenza non esclusiva per l'esercizio dei diritti di riproduzione e adattamento inerenti ai video caricati sia la possibilità per l'ISP di rimuoverli; – il *provider* che fornisca un servizio automatico di "video correlati" consistente nella visualizzazione a lato o sotto il video in riproduzione di altri contenuti a esso associabili in qualche modo».

[45] Si tratta, a ben vedere, di una scelta che muove dall'idea che, all'apparire di una rivoluzione economica segnata dalla nascita di un nuovo mercato, il legislatore non possa discostarsi dalle regole ordinarie della responsabilità civile´ fondate sul principio della colpa´ , trattandosi di un sistema indubbiamente meno gravoso rispetto ad altri regimi giuridici, che, pertanto, favorisce l'iniziativa economica ed il decollo degli operatori del mercato nascente. In tale prospettiva, è solo dopo l'affermarsi del settore e con il pieno dispiegarsi delle risorse economiche degli operatori, che gli ordinamenti giuridici avrebbero la possibilità di imporre agli imprenditori del settore´ per ragioni di equità e solidarietà´ regole sempre maggiori di responsabilità connesse al rischio di impresa nel settore o, addirittura, regole di responsabilità oggettiva. Sul punto, Bocchini (2017), p. 636.

[46] La categoria dell'*hosting* attivo ha, d'altra parte, trovato un riconoscimento anche da parte della Corte di Giustizia UE, la quale ha evidenziato la necessità di valorizzare, al fine dell'applicabilità o meno del regime di irresponsabilità sancito dalla direttiva sull'*e-commerce*, il concreto *modus operandi* degli Isp. In particolare, secondo i giudici europei, l'esenzione di responsabilità del *provider* per il contenuto illecito dei fatti postati dagli utenti in rete, si riferisce esclusivamente alle piattaforme digitali prive di un ruolo attivo nella gestione dei contenuti, che gli permetta di avere conoscenza o controllo dei dati memorizzati: Corte di Giustizia UE, 23 marzo 2010, C-236/08, C-237/09, C-238/08, *Google Inc. c. Louis Vuitton e altri*.

di prospettiva, permangono numerose perplessità rispetto alla possibilità di configurare una responsabilità del *provider* strutturata secondo il modello del reato omissivo improprio.

Invero, in assenza di una norma generale di incriminazione suppletiva che stabilisca una clausola di equivalenza tra il non interrompere gli effetti di un reato e la sua realizzazione commissiva – sulla falsariga di quanto previsto dall'art. 40 cpv c.p. –, non sembra possibile imputare un soggetto per non aver interdetto la protrazione dell'offesa al bene giuridico, pena la violazione del principio di legalità in materia penale[47].

Non solo. La responsabilità per omesso impedimento del reato presuppone, a ben vedere, che questo non sia stato già consumato[48]; circostanza che, nel delitto di diffamazione *online*, si realizza – per pacifica giurisprudenza – nel momento in cui l'autore delle espressioni illecite attiva il collegamento[49].

Non pare, dunque, possibile ravvisare una partecipazione del *provider* – ancorché nella forma omissiva – alla condotta diffamatoria, avuto riguardo sia al successivo mantenimento della disponibilità in rete dei contenuti, sia alla loro omessa cancellazione, trattandosi di condotte susseguenti all'avvenuta realizzazione del reato[50].

3.1. *(segue) Gli obblighi di rimozione successivi alla commissione del reato: quale modello sanzionatorio per l'ISP?*

La non persuasività del modello idealtipico fondato sul reato omissivo improprio non deve, tuttavia, essere intesa come accettazione del paradigma opposto, che esclude ogni forma di responsabilità in capo all'Isp, ad eccezione dei casi di autoria o co-autoria nella realizzazione del reato. Una tale impostazione sottovaluta, infatti, il contributo che il *provider* offre nella diffusione dei contenuti digitali illeciti, tanto nella fase iniziale della loro immissione in rete, quanto in quella successiva della loro permanenza, ancor più ove si tenga conto della funzione sempre più attiva che caratterizza la loro attività.

D'altra parte, che il modello della generale "irresponsabilizzazione", sancito anche dal legislatore, non sia più in linea con l'attuale evoluzione tecnologica emerge chiaramente – come si è visto – guardando ai mutamenti interpretativi della giurisprudenza.

Preso, dunque, atto della parziale inadeguatezza del testo normativo di riferimento, una rielaborazione delle regole fondanti la responsabilità del *provider* non può che concentrarsi sulla fase successiva a quella del caricamento del contenuto illecito da parte degli utenti, valorizzandone – nell'ottica di un bilanciamento tra la libertà di impresa dell'Isp, la libertà di espressione dell'utente e la tutela dei terzi – il ruolo di "tutore dell'ordine".

In questa prospettiva, sarebbe auspicabile la previsione di uno specifico obbligo inerente alla rimozione dei contenuti illeciti o all'inibizione dell'accesso agli utenti ai siti che li contengano, sulla falsariga delle disposizioni dettate in materia di tutela del diritto d'autore e di contrasto alla diffusione di materiale pedopornografico e al terrorismo[51].

Sennonché, anche nell'ottica di una siffatta regolamentazione, permangono alcuni punti critici.

Il primo – già *de jure condito* particolarmente problematico – attiene all'individuazione del momento in cui scatta l'obbligo di rimozione in capo all'Isp e, più specificamente, se sia ne-

[47] Così, Ingrassia (2017), p. 1627.
[48] Così, Ingrassia (2017), p. 1625.
[49] Cfr., Cass. pen., sez. V, 21 giugno 2006, n. 25875, Cicino, in CED 234528; Cass. pen., sez. V, 4 aprile 2008, n. 16262, T.E.N., in www.iusexplorer.it.
[50] Si tratta, a ben vedere, di un'impostazione che, secondo una parte della dottrina, riguarda tutti i reati fondati su verbi modali, come diffondere o divulgare, che, consumandosi nel momento in cui i contenuti illeciti sono resi accessibili da parte del loro autore, non possono ravvisare una partecipazione del provider «né nel successivo mantenimento della disponibilità in rete di quei contenuti, né nella loro omessa cancellazione, in entrambi i casi trattandosi di condotte susseguenti la già avvenuta realizzazione del reato»: così, Seminara (1998), p. 765; Flor (2010), p. 462 ss.; Ingrassia (2012), p. 21 ss.; Id. (2017), p. 1625.
[51] Il riferimento è, in particolare, ai già citati meccanismi di c.d. *notice and take down* previsti per tali settori di materia dal legislatore, in forza dei quali il *provider* è tenuto ad informare dei contenuti dalla dubbia liceità l'autorità competente, che farà le proprie valutazioni e, eventualmente, comunicherà un ordine di rimozione o imporrà di inibire l'accesso agli utenti.
Si tratta, peraltro, di uno strumento che è stato recentemente riproposto – seppure senza affiancare un sistema sanzionatorio *ad hoc* – anche in relazione al tentativo di arginare il fenomeno del c.d. cyberbullismo. L'art. 2 della L. 29 maggio 2017, n. 71, prevede, infatti, la possibilità per il minore ultraquattordicenne – o per il genitore ovvero per il soggetto responsabile –, vittima di uno degli illeciti riconducibili *ex* art. 1, comma 2, della stessa legge, di inoltrare al titolare del trattamento o al gestore del sito internet un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore stesso diffuso in Internet. Sul punto, in senso parzialmente critico, per tutti, Panattoni (2018), p. 260.

cessario un provvedimento o una comunicazione dell'Autorità o, piuttosto, se sia sufficiente la mera conoscenza del contenuto illecito, ottenuta, ad esempio, attraverso una notifica effettuata dalla parte offesa.

Ora, fermi i casi in cui è lo stesso legislatore a dare indicazioni dirimenti, la questione non risulta di agevole soluzione: invero, appare evidente che rimettere l'individuazione del momento in cui scatta l'obbligo di rimozione a informazioni acquisite autonomamente dallo stesso *provider* o a comunicazioni provenienti da soggetti privati, rischia di riproporre gli inconvenienti del modello di responsabilità fondato su un controllo censorio *ex ante*[52]; tuttavia, non può negarsi come le velocissime dinamiche del *web* non consentano sempre di attendere le più lente procedure formali della giustizia[53].

Il secondo – decisivo – profilo di criticità riguarda, invece, il tipo di conseguenze che dovrebbero essere ascritte al *provider* in caso di mancata ottemperanza degli obblighi che gli impongono di rimuovere i contenuti illeciti o di inibire l'accesso ai siti web che li contengono.

Guardando alle disposizioni già esistenti, deve osservarsi come, a fronte di alcuni casi in cui è la stessa legge a stabilire il regime sanzionatorio dell'inadempimento, prevedendo una sanzione amministrativa pecuniaria[54], ve ne siano altri – caratterizzati dal silenzio del legislatore[55] – rispetto ai quali è stata prospettata l'applicazione del delitto di inosservanza dolosa del provvedimento del giudice (art. 388 c.p.) 56 o della contravvenzione di inosservanza dei provvedimenti dell'Autorità (art. 650 c.p.)[57]

Si tratta, tuttavia, di soluzioni poco soddisfacenti. A ben vedere, infatti, l'applicazione di

[52] Così, *ex plurimis*, Bartoli (2013), p. 606; Ingrassia (2017), p. 1628; Carbone (2017), p. 2784. Al rischio di attribuire nuovamente al *provider* il ruolo di censore, quest'ultimo Autore affianca, altresì, quello dell'incidenza sul carico giudiziario delle Procure: il timore di incorrere in un addebito penale per i casi di inerzia, potrebbe, infatti, portare gli operatori a riversare ogni comunicazione sospetta sugli uffici giudiziari.

[53] Si tratta di una posizione recentemente sostenuta sia dalla giurisprudenza di merito che da quella di legittimità, quantomeno con riferimento alle attività di *hosting*: cfr., Trib. Napoli Nord, sez. II, 3 novembre 2016, cit., nonché Cass. pen., sez. V, 27 dicembre 2016, n. 54946, cit. In particolare, secondo i giudici partenopei, la non indispensabilità di un ordine specifico dell'autorità per la rimozione dell'attività e/o dell'informazione illecita deriverebbe dalle seguenti argomentazioni: «1. Dall'articolazione del regime di esonero dalla responsabilità in due fattispecie distinte (lettere a e b del comma 1 dell'art. 16) laddove, se si fosse voluto ritenere nascente l'obbligo di rimozione dal solo ordine delle autorità competenti, non avrebbe avuto senso alcuno prevedere un'ipotesi autonoma di "irresponsabilità" connessa, semplicemente, alla non effettiva "conoscenza del fatto che l'attività o l'informazione è illecita"; 2. Dalla stessa previsione di cui al successivo art. 17 nel senso che, se l'obbligo di rimozione può derivare solo da un precedente ordine dell'autorità, non ci sarebbe motivo di sancire l'assenza di un generale obbligo di sorveglianza giacché, in ogni caso, il provider non potrebbe o, comunque, non dovrebbe attivarsi spontaneamente o volontariamente per impedire l'attività e la diffusione dell'informazione illecita; 3. Dallo stesso tenore letterale dell'art. 17 il quale nel sancire l'assenza di un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite consente di ritenere che un obbligo di tal fatta sussista a fronte di una conoscenza acquisita "passivamente" (ossia a seguito di specifica denuncia o segnalazione proveniente da terzi soggetti) ed in modo specifico (ovvero con indicazione delle attività e/o delle informazioni illecite); 4. Dal tenore letterale dei "considerando" nn. 42 e ss. della stessa dir. 2000/31/CE e, in particolare, del n. 46 secondo cui "Per godere di una limitazione della responsabilità, il prestatore di un servizio della società dell'informazione consistente nella memorizzazione di informazioni deve agire immediatamente per rimuovere le informazioni o per disabilitare l'accesso alle medesime non appena sia informato o si renda conto delle attività illecite (…)"; 5. Dalla valutazione degli interessi coinvolti giacché, venendo in rilievo diritti della personalità (quali l'immagine, il decoro, la reputazione, la riservatezza), appare irrazionale dover attendere un ordine dell'autorità il quale potrebbe intervenire quando ormai i diritti in questione sono irrimediabilmente pregiudicati e non più suscettibili di reintegrazione; 6. dall'esigenza di bilanciare gli interessi in conflitto (garantire la diffusività e la capillarità delle comunicazioni e tutelare la sfera personale degli interessati) sicché il punto di equilibrio può ragionevolmente essere rinvenuto in un sistema di controllo successivo ed attivazione precipua da parte del soggetto titolare dei diritti della personalità ritenuti violati».
Dello stesso avviso è la giurisprudenza della Corte di Giustizia, 12 luglio 2011, C-324/09, *L'Oreal e altri c. eBay International*, cit., la quale ha affermato che «è sufficiente, affinché il prestatore di un servizio della società dell'informazione non possa fruire dell'esonero dalla responsabilità previsto all'art. 14 della direttiva 2000/31, che egli sia stato al corrente di fatti o di circostanze in base ai quali un operatore economico diligente avrebbe dovuto constatare l'illiceità di cui trattasi (…). Inoltre, affinché non siano private del loro effetto utile, le norme enunciate all'art. 14, n. 1, lett. a), della direttiva 2000/31 devono essere interpretate nel senso che riguardano qualsiasi situazione nella quale il prestatore considerato viene ad essere, in qualunque modo, al corrente di tali fatti o circostanze. Sono quindi contemplate, segnatamente, la situazione in cui il gestore di un mercato *online* scopre l'esistenza di un'attività o di un'informazione illecite a seguito di un esame effettuato di propria iniziativa, nonché la situazione in cui gli sia notificata l'esistenza di un'attività o di un'informazione siffatte. In questo secondo caso, pur se, certamente, una notifica non può automaticamente far venire meno il beneficio dell'esonero dalla responsabilità previsto all'art. 14 della direttiva 2000/31 – stante il fatto che notifiche relative ad attività o informazioni che si asseriscono illecite possono rivelarsi insufficientemente precise e dimostrate –, resta pur sempre fatto che essa costituisce, di norma, un elemento di cui il giudice nazionale deve tener conto per valutare, alla luce delle informazioni così trasmesse al gestore, l'effettività della conoscenza da parte di quest'ultimo di fatti o circostanze in base ai quali un operatore economico diligente avrebbe dovuto constatare l'illiceità».

[54] Il riferimento è alla già citata disciplina dettata dall'art. 14 *quater*, L. 3 agosto 1998, n. 269, in materia di contrasto alla diffusione di materiale pedopornografico, la quale prevede l'applicazione di una sanzione amministrativa pecuniaria da euro 50.000 a euro 250.000, irrogata dal Ministero delle comunicazioni. Analogamente dispone l'art. 1, comma 7, D.L. 22 marzo 2004, n. 72 (convertito con l. 21 maggio 2004, n. 128), per i casi di violazione del diritto d'autore.

[55] Si pensi, esemplificativamente, alla citata normativa prevista dell'art. 2 D.L.18 febbraio 2015, n. 727, che, per il caso di mancato adempimento all'ordine di rimozione dei contenuti illeciti disposto dal Pubblico Ministero, si limita a stabilire la sola sanzione dell'interdizione dell'accesso al dominio internet.

[56] Così, Spagnoletti (2004), p. 1929 ss.

[57] In questo senso, Ingrassia (2012), p. 38; E. La Rosa (2016), p. 739 ss.

tali fattispecie richiede l'esistenza di un provvedimento dell'Autorità – presupposto la cui necessità, come si è detto, non risulta affatto pacifica[58] –; nonché, con specifico riferimento all'art. 388 c.p., il compimento di atti fraudolenti, che, secondo la prevalente dottrina e giurisprudenza, non possono rinvenirsi nella mera inosservanza della decisione giudiziaria[59].

A ciò si aggiunga, poi, l'incongruenza sistematica che si determinerebbe nell'applicare, per i casi caratterizzati dal silenzio del legislatore, la sanzione penale, per quelli espressamente disciplinati dalla legge, la sanzione amministrativa[60].

L'auspicio non può che essere, allora, quello di un'armonizzazione della risposta dell'ordinamento a fronte delle condotte omissive dell'Isp; armonizzazione che, tuttavia, presuppone la risoluzione della preliminare questione inerente all'opportunità di far leva, per tali ipotesi, sulla sanzione penale.

In questa prospettiva, ci sembra maggiormente condivisibile l'opinione di chi ritiene che sarebbe da preferire il ricorso a sanzioni amministrative pecuniarie, anche elevate, eventualmente accompagnate da sanzioni interdittive[61]: la predisposizione di un modello sanzionatorio fondato sulla risposta amministrativa risulta, infatti, per un verso, maggiormente rispettoso dei principi di proporzione e sussidiarietà dell'intervento penale, evitando il rischio di un suo uso meramente simbolico; per l'altro, appare dotato di una più intensa efficacia dissuasiva, trattandosi di fatti commessi da soggetti che, generalmente, gestiscono un'attività d'impresa, pertanto, particolarmente sensibili all'incidenza patrimoniale della sanzione, nonché a risposte di carattere inibitorio.

4. La responsabilità del *provider* per i discorsi d'odio: l'esperienza tedesca per "migliorare la tutela dei diritti sui *social network*".

I nodi dogmatici fin qui evidenziati risultano ancora più intricati ove ci si focalizzi sul tema da cui è partita questa riflessione, ossia i discorsi d'odio.

Invero, non può non cogliersi la problematicità del rimettere, in via esclusiva, a un soggetto privato la valutazione delle manifestazioni del pensiero effettivamente riconducibili all'*hate speech*, non solo per il rischio che siffatta valutazione sia mossa essenzialmente per assecondare i propri interessi economici, ma soprattutto perché il *provider* non sembra dotato degli strumenti culturali necessari per emettere un tale giudizio[62].

A ciò si aggiunga la già evidenziata criticità in ordine alla possibilità di utilizzare lo strumento penale per criminalizzare i discorsi d'odio, la quale non può che traslarsi sulla configurazione della responsabilità in capo al *provider* per la mancata rimozione di questo tipo di contenuto illecito.

Quale, dunque, la soluzione? Come si è già detto, non convince l'idea di una generale irresponsabilità dei *provider*, stante il ruolo che questi rivestono nella permanenza e nella diffusione dell'odio online; ruolo ancor più accentuato ove la sua attività non si limiti ad una memorizzazione passiva, come nel caso dei *social network*. Occorre piuttosto individuare specifici meccanismi che, a fronte dell'auspicata responsabilizzazione per i casi di mancata rimozione dei messaggi offensivi, consentano un efficace bilanciamento degli interessi coinvolti.

Sotto questo profilo, alcuni spunti interessanti provengono dalla recente normativa introdotta in Germania, entrata in vigore il 1° ottobre 2017, che si propone di contrastare gli abusi realizzati sui *social network* e, più in particolare, la diffusione dei discorsi d'odio e delle *fake news*[63].

[58] Così, E. La Rosa (2016), p. 740.
[59] In questo senso, già, Marini (1959), p. 1218 ss.; Pazienza (1979), p. 81 ss.; Alessandri (1981), p. 154 ss. Più recentemente, Bisori (2008), p. 673 ss.; Mannucci Pacini (2015), p. 1354 ss.; Romano (2016), p. 325 ss.; Piffer (2017), p. 1224 ss.; nonché, nella manualistica, Fiandaca – Musco (2012), p. 433 – 434. In giurisprudenza, *ex multis*, Cass. pen., sez. VI, 13 febbraio 2006, n. 17543, S.F., in *Riv. pen.*, 2007, p. 180 ss.; Cass. pen., sez. Un., 27 settembre 2007, n. 36692, V.G., in *Guid. dir.*, 2007, n. 46, p. 81 ss.; Cass. pen., sez. VI, 4 maggio 2010, n. 23274, G.R., in *Guid. dir.*, 2010, n. 35, p. 66 ss.
[60] Così, Ingrassia (2012), p. 38; E. La Rosa (2016), p. 740.
[61] In questo senso, Ingrassia (2012), p. 40-41; E. La Rosa (2016), p. 740.
[62] Così, già, Fornasari (2004), p. 431, secondo cui «è inquietante, in sostanza, l'idea di un privato che verrebbe incaricato di esercitare una sorta di censura per conto dell'ordinamento, avendo i mezzi tecnici ma non quelli culturali per realizzarla».
[63] Il riferimento è, più specificamente, alla nuova "Legge per migliorare la tutela dei diritti sui *social network*" (*Netzwerkdurchsetzungsgesetz – NetzDG*), entrata in vigore nella Repubblica federale tedesca il 1° ottobre 2017, il cui articolato, tradotto in lingua italiana, è consultabile in *Dir. info.*, 2017, p. 723 ss. Obiettivo della legge è, evidentemente, quello di contrastare il linguaggio d'odio on line ed ogni forma di discriminazione

In particolare, la nuova disciplina prevede – tra gli altri – l'obbligo, per le piattaforme *social* aventi almeno due milioni di utenti registrati in Germania, di predisporre un sistema di notifica dei contenuti illeciti efficace e facilmente accessibile agli utenti[64]. Tale sistema deve garantire che il gestore del *social network* si occupi immediatamente della segnalazione, rimuovendo i contenuti segnalati entro 24 ore se manifestamente illeciti[65]; entro 7 giorni negli altri casi, salva la possibilità di rivolgersi a un apposito organismo di autoregolamentazione accreditato[66].

A tale previsione si affianca, poi, l'obbligo di garantire una procedura trasparente per la gestione delle segnalazione, che informi l'utente che ha pubblicato i contenuti, nonché colui che ha effettuato la segnalazione, della decisione adottata e delle sue motivazioni. Il soggetto che si reputa leso da contenuti non rimossi o disabilitati può rivolgersi al giudice di merito, la cui decisione non è impugnabile[67].

Il mancato rispetto della disciplina comporta l'applicazione di una sanzione amministrativa pecuniaria, il cui importo massimo può variare tra i cinquecento mila euro e cinque milioni di euro, a seconda del tipo di violazione.

Alla luce di questa sintesi, ci sembrano diversi i meriti che possono riconoscersi all'approccio normativo avviato in Germania. Anzitutto, risulta significativa la scelta di intervenire con una normativa giuridicamente vincolante, anziché con un sistema di autoregolamentazione, per contrastare il perpetrarsi di fattispecie fortemente lesive di beni attinenti alla persona e alla collettività (onore, reputazione, riservatezza, dignità, uguaglianza, non discriminazione)[68].

Secondariamente, appare apprezzabile l'equilibrio raggiunto nel bilanciare i diversi interessi coinvolti, in considerazione della possibilità di rivolgersi a un organo di autoregolamentazione indipendente; della presenza di strumenti finalizzati a garantire il contraddittorio delle parti; ma, soprattutto, della differenziazione delle tempistiche degli obblighi di rimozione: alla luce della già evidenziata carenza di attitudini intellettuali e culturali del *provider* nel discernimento dell'illiceità delle informazioni che transitano sui loro *server*, risulta, infatti, particolarmente meritevole la scelta di assicurare un più ampio lasso temporale per intervenire su quei contenuti che non sono manifestamente inquadrabili nella categoria dell'*hate speech* e che, pertanto, richiedono una più attenta ponderazione al fine di scongiurare forme di censura arbitraria[69].

Da ultimo, ci pare potersi guardare con favore anche al modello sanzionatorio prescelto: in primo luogo perché le sanzioni si focalizzano sull'inottemperanza degli obblighi imposti al *provider*, senza contemplare in maniera espressa il fatto che la decisione sul merito della segnalazione, quindi sull'illiceità del contenuto, possa risultare erronea, ridimensionando così i rischi di pretese risarcitorie[70]; in secondo luogo, per la scelta di utilizzare una sanzione punitiva amministrativa, peraltro piuttosto elevata, anziché quella penale.

basata sull'opinione, sul colore della pelle, sull'etnia, sulla religione, sulle tendenze sessuali e, più in generale, tutti i comportamenti illeciti diffusi sui social media, compresa la diffusione di notizie false: cfr., la relazione di accompagnamento alla proposta di legge (*Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzungin sozialen Netzwerken*) in http://dipbt.bundestag.de/dip21/btd/18/127/1812727.pdf.
Per un commento alla disciplina, Codiglione (2017), p. 728 ss.

[64] La legge non appresta una definizione generica di "contenuto illecito", ma richiama un vasto insieme di norme del Codice penale tedesco in tema di utilizzo di simboli e propaganda politica vietata (§§ 86, 86a), preparazione ed incitamento alla commissione di gravi crimini contro lo Stato (§§ 89a, 91), falso per l'alto tradimento dello Stato (§100a), pubblico incitamento alla violenza (§ 111), disturbo della pace pubblica con la minaccia di crimini (§ 126), associazione criminale o terroristica (§§ 129, 129b), sedizione (§ 130), diffusione di contenuti violenti (§131), ricompensa e approvazione di crimini (§ 140), diffamazione religiosa o ideologica (§ 166), distribuzione, acquisto o detenzione di materia pedopornografico (§184b), comunicazione al pubblico di contenuto pornografici (§ 184d), violazione della riservatezza attraverso la creazione o la diffusione di fotografie (§201a), ingiuria, calunnia e diffamazione (§§ 185-187), minaccia (§241) e falsificazione di prove (§269).

[65] Salvo che il *social network* abbia concordato con l'autorità giudiziaria competente un periodo più lungo (§3, comma 2).

[66] In particolare, la decisione di accreditamento è presa dall'Ufficio Federale di giustizia, allorché l'organismo «1. Assicuri l'indipendenza e le capacità tecniche delle proprie risorse; 2. Offra mezzi adeguati per garantire una valutazione rapida entro 7 giorni; 3. Abbia adottato norme di procedura che regolino lo scopo e durata della valutazione, stabiliscano i requisiti di ammissione dei *social network* affiliati e prevedano la possibilità di riesaminare le decisioni; 4. Abbia adottato un servizio di ricezione delle segnalazioni; 5. Sia finanziato da diversi gestori di *social network* o istituzioni garantendo la disponibilità di mezzi adeguati. L'organismo deve rimanere aperto all'adesione di altri prestatori di servizi e in particolare di *social network*».
Il termine di sette giorni può essere, altresì, superato se la decisione sull'illiceità del contenuto dipende dalla falsità di una dichiarazione o da circostanze di fatto (§3, comma 3).

[67] La decisione così emessa è vincolante per l'autorità amministrativa tenuta a irrogare la sanzione (§ 4, comma 5).

[68] In questo senso, Codiglione (2017), p. 732.

[69] In questo senso, Panattoni (2018), p. 259.

[70] Evidenzia tale profilo, Codiglione (2017), p. 732. Si tratta, a ben vedere, di una soluzione che attenua i rischi di quello che è stato definito come c.d. "dilemma del *provider*": a fronte di una diffida a rimuovere un'informazione da parte di un soggetto che si assuma danneggiato, l'Isp si trova esposto davanti alla difficile alternativa di assecondare l'intimazione, esponendosi al rischio di pretese risarcitorie da parte dell'utente che dimostri la liceità dell'informazione rimossa o, al contrario, di non rimuovere il contenuto asserito come illecito, esponendosi però alla pretesa risarcitoria dell'intimante che provi l'effettiva illiceità del materiale non eliminato. Sul punto, per tutti, Bartoli (2013), p. 606.

5. Considerazioni conclusive.

L'analisi fin qui effettuata ha messo in luce la necessità di una più puntuale regolamentazione delle attività che interessano il Cyberspazio, soprattutto in considerazione del ruolo sempre più attivo che i *provider* svolgono, e della sempre maggiore incisività che i sistemi *online* hanno sulle nostre vite.

Tale necessità appare ancor più preminente ove si guardi alla pervasiva diffusione delle manifestazioni d'odio sul *web*: come si è visto, il potenziale comunicativo di internet ha aperto la strada alla pubblicità degli istinti più nascosti, determinando una progressiva e incessante proliferazione dell'odio. Basta frequentare un qualunque *social network* per rendersi conto di come, nel corso degli anni, i toni siano cambiati.

Si tratta, peraltro, di un cambiamento che coinvolge tutti i livelli di comunicazione, ivi compreso quello politico e istituzionale: l'odio genera potenza coesiva, consente di mobilizzare le masse e ottenere consenso[71].

Il ripensamento delle regole di responsabilità degli intermediari della rete non può, tuttavia, prescindere da un'attenta ponderazione dei diversi interessi in gioco, soprattutto ove si intenda sollecitare l'intervento del legislatore penale.

In questa prospettiva, va certamente scongiurata ogni forma di eccessiva criminalizzazione del *web*: una legislazione liberticida dell'ecosistema digitale – ancorché finalizzata alla tutela dell'uguaglianza e della dignità degli individui – rischia non solo di determinare un'inaccettabile compressione della libertà di manifestazione del pensiero; ma, soprattutto, di alterare i comportamenti e le preferenze degli utenti, nonché le strategie commerciali delle piattaforme tecnologiche, con pesanti conseguenze dal punto di vista economico[72].

Ben più equilibrata appare, piuttosto, la previsione di sistemi regolatori, legalmente vincolanti, che impongano ai *provider* obblighi di rimozione successivi, accompagnati da specifiche garanzie, quali la certezza e la brevità delle tempistiche, la trasparenza delle procedure, il rispetto del contraddittorio, sulla scorta di quanto già prescritto – come si è visto – in alcuni Paesi europei.

L'effettività di una regolamentazione siffatta potrà, però, essere garantita solo ove inserita nel quadro di una più ampia armonizzazione della legislazione sovranazionale – se non addirittura internazionale –: l'eterogeneità e la frammentarietà degli approcci normativi non può, infatti, che favorire la perpetrazione delle condotte offensive, stante la natura atemporale e a-spaziale del *web*.

I recenti sforzi compiuti a livello eurounitario nel senso di favorire una collaborazione con le piattaforme digitali e di elaborare codici di condotta rappresentano, certamente, un primo passo in tale direzione. Più in generale, è da salutare con favore l'attenzione sempre più di frequente riservata, nel disciplinare materie "sensibili", al ruolo del *provider* – sia sufficiente richiamare le già menzionate direttive in materia di tutela del diritto d'autore o di contrasto al terrorismo – nella consapevolezza che lo stesso, a fronte di una sempre più ampia varietà di servizi offerti, non abbia più un ruolo meramente tecnico e passivo.

La strada insomma inizia ad essere tracciata. Si tratta di proseguire con decisione nel cammino non semplice, ma necessario, della progressiva armonizzazione delle regole.

[71] Sul tema, più ampiamente, Ziccardi (2016), p. 229 ss.

[72] Sotto questo profilo, ha suscitato alcune perplessità tra i titolari delle piattaforme *web* la proposta di direttiva sul diritto d'autore nel mercato unico digitale, avanzata dalla Commissione europea e attualmente in discussione al Parlamento, il cui obiettivo è quello di armonizzare il quadro normativo comunitario in materia di diritto d'autore nell'ambito delle tecnologie digitali. In particolare, è stata oggetto di diverse critiche la disposizione contenuta all'art. 13 dell'articolato, la quale prevede l'obbligo per i *provider* di adottare misure miranti impedire che le opere, o altro materiale, coperto dal diritto d'autore siano messi a disposizione sui loro servizi, anche attraverso il ricorso a tecnologie di riconoscimento dei contenuti. Si tratta – secondo i suoi detrattori – di una norma che, di fatto, impone ai prestatori di servizi informatici l'adozione di un sistema di controllo preventivo sul materiale pubblicato *online*, ponendosi, pertanto, in aperto contrasto con quanto fino a oggi previsto dalla direttiva sul commercio elettronico e dalla giurisprudenza della Corte di Giustizia, nonché, più in generale, con il principio di libera circolazione delle informazioni in rete. Cfr., *Perché la direttiva Ue sul copyright potrebbe significare la morte di Internet come lo conosciamo*, in *The Post International*, 13 settembre 2018.
Il testo della proposta di direttiva è consultabile su https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52016PC0593.

Bibliografia

Alessandri, Alberto (1981): "*Il problema delle misure coercitive e l'art. 388 c.p.*", *Riv. it. dir. proc. pen.*, p. 154 ss.

Ambrosetti, Enrico Mario (2006): "*Beni giuridici tutelati e struttura delle fatti-specie: aspetti problematici nella normativa penale contro la discriminazione razziale*", in Riondato, Silvio (eds.) (2006), p. 93 ss.

Bartoli, Roberto (2013): "*Brevi considerazioni sulla responsabilità penale dell'*Internet Service Provider", *Dir. pen. proc.*, p. 600 ss.

Birritteri, Emanuele (2017): "*Diffamazione e* Facebook: *la Cassazione conferma il suo indirizzo ma apre a un'estensione analogica* in malam partem *delle norme sulla stampa*", *Dir. pen. cont.*, 20 aprile 2017.

Bisori, Luca (2008): "*La mancata esecuzione dolosa di provvedimenti del giudice*", in Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo, Papa, Michele (eds.) (2008), p. 673 ss.

Bocchini, Roberto (2017): "*La responsabilità di* Facebook *per la mancata rimozione dei contenuti illeciti*", Giur. it., p. 629 ss.

Brunelli, David (2016): "*Attorno alla punizione del negazionismo*", *Riv. it. dir. proc. pen.*, p. 978 ss.

Buffa, Francesco (2017): "*Responsabilità del gestore del sito* internet", *Questione Giustizia* (9 gennaio 2017).

Bugiolacchi, Leonardo (2017): "*I presupposti dell'obbligo di rimozione dei contenuti da parte dell'*hosting provider *tra interpretazione giurisprudenziale e dettato normativo*", *Resp. civ. prev.*, p. 536 ss.

Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo, Papa, Michele (2008): *Trattato di diritto penale. Parte Speciale*, vol. III, (Torino, Giappichelli).

Caggiano, Giandonato (2014): *Percorsi giuridici per l'integrazione. Migranti e titolari di protezione interna internazionale tra diritto dell'Unione e ordinamento italiano*, (Torino, Giappichelli).

Caputo, Matteo, (2014): "*La "menzogna di Auschwitz", le "verità" del diritto penale. La criminalizzazione del c.d. negazionismo tra ordine pubblico, dignità e senso di umanità*", *Dir. pen. cont.*, 7 gennaio 2014, ora anche in Forti, Gabrio, Varraso, Gianluca, Caputo, Matteo (2014): "*"Verità" del precetto e della sanzione penale alla prova del processo*", (Napoli, Jovene), p. 63 ss.

Carbone, Roberto (2017): "*Responsabilità del* Blogger: *parziale* rivirement *della Cassazione?*", *Cass. pen.*, p. 2782 ss.

Cassano, Margherita (2014): "*Negazionismo e opportunità di una risposta penale*", *Criminalia – Annuario di scienze penalistiche - 2013*, (Pisa, ETS), p. 279 ss.

Cavaliere, Antonio (2016): "*La discussione intorno alla punibilità del negazionismo. I principi di offensività e libera manifestazione del pensiero e la funzione della pena*", *Riv. it. dir. proc. pen.*, p. 999 ss.

Codiglione, Giorgio Giannone (2017): "*La nuova legge tedesca per l'*enforcement *dei diritti sui social media*", *Dir. info.*, p. 728 ss.

Corbetta, Stefano (2014): "*Caso* "Google": *nessuna responsabilità dell'*"Host provider" *per l'omesso impedimento dei reati realizzati dagli utenti della rete*", *Dir. pen. proc.*, p. 277 ss.

Corrias Lucente, Giovanna (2004): "*Ma i* network providers*, i* service providers *e gli* access providers *rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che loro gestiscono?*", *Giur. mer.*, p. 2523 ss.

Corrias Lucente, Giovanna (2015): "*Le testate telematiche registrate sono sottratte al sequestro preventivo. Qualche dubbio sulla "giurisprudenza legislativa"*", *Dir. info.*, p. 1041 ss.

Costanzo, Pasquale (2000): "*Ancora a proposito dei rapporti tra diffusione in Internet e pubblicazione a mezzo stampa*", *Dir. info.*, p. 657 ss.

De Flammineis, Siro (2016): "*Riflessioni sull'aggravante del "negazionismo": offensività della condotta e valori in campo*", Dir. pen. cont., 17 ottobre 2016.

De Francesco, Giovannangelo (1994): "*Commento all'art. 1 D. L. n. 122/93 conv. con modifiche dalla l. n. 205/93*", *Leg. pen.*, p. 174 ss.

De Natale, Domenico (2009): "*La responsabilità dei fornitori di informazioni in internet per i casi di diffamazione* on line", *Riv. trim. dir. pen. econ.*, p. 539 ss.

Di Ciommo, Francesco (2017): "*Responsabilità dell'*internet hosting provider, *diffamazione a mezzo* Facebook *e principio di tassatività della norma penale: troppa polvere sotto il tappeto*", *Foro it.*, p. 251 ss.

Di Giovine, Alfonso (2005): *Democrazie protette e protezione della democrazia*, (Torino, Giappichelli).

Di Giovine, Alfonso (2006): "*Il passato che non passa: "Eichmann di carta" e repressione penale*"", *Riv. dir. pubbl. comp. eur.*, 1, p. XIII.

Diotallevi, Lorenzo (2015): "*La Corte di cassazione sancisce l'"equiparazione" tra giornali cartacei e telematici ai fini dell'applicazione della disciplina in materia di sequestro preventivo: un nuovo caso di "scivolamento" dalla "nomofilachia" alla "nomopoiesi"?*", *Giur. cost.*, p. 1055 ss.

Dolcini, Emilio (2011): "*Di nuovo affossata una proposta di legge sull'omofobia*", *Dir. pen. proc.*, p. 1393 ss.

Dolcini, Emilio (2014): "*Omofobi: nuovi martiri della libertà di manifestazione del pensiero?*", *Riv. it. dir. proc. pen.*, p. 7 ss.

Dolcini, Emilio, Gatta, Gian Luigi (2015): *Codice penale commentato*, vol. II (Milano, Giuffrè).

Fiandaca, Giovanni, Musco, Enzo (2012): *Diritto penale. Parte Speciale*, vol. I, V ed., (Bologna, Zanichelli).

Fiandaca, Giovanni, Musco, Enzo (2014): *Diritto penale. Parte generale*, VII ed., (Bologna, Zanichelli).

Flor, Roberto (2010): *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di internet. Un'indagine comparata in prospettiva europea e internazionale*, (Padova, Cedam).

Fornari, Luigi (2007): voce *Discriminazione razziale*, in Palazzo, Francesco, Paliero, Carlo Enrico (eds.) (2007), p. 1034 ss.

Fornasari, Gabriele (2004): "*Il ruolo dell'esigibilità nella definizione della responsabilità penale del* provider", in Picotti, Lorenzo (eds.) (2004), p. 423 ss.

Forti, Gabrio, Seminara, Sergio, Zuccalà, Giuseppe (2017): *Commentario breve al codice penale*, (Milano, Giuffrè).

Fronza, Emanuela (1997): "*Osservazioni sull'attività di propaganda razzista*", *Riv. int. dir. uomo*, p. 32 ss.

Fronza, Emanuela (2012): *Il negazionismo come reato*, (Milano, Giuffrè).

Fronza, Emanuela (2017): "*L'introduzione dell'aggravante di negazionismo*", *Dir. pen. proc.*, p. 155 ss.

Gardaglione, Iginio, Danit, Gal, Alvez, Thiago, Martinez,Gabriela (2015): Countering online hate speech, (Parigi, Unesco Publishing).

Gasparini, Irene (2017): "*L'odio ai tempi della rete: le politiche europee di contrasto all'*online hate speech", *Jus*, p. 505 ss.

Goisis, Luciana (2012): "*Omofobia e diritto penale: profili comparatistici*", *Dir. pen. cont.*, 16 novembre 2012.

Goisis, Luciana (2015): "*Omosessualità*, hate crimes *e diritto penale*", *GenIUS*, 1, p. 40 ss.

Gullo, Antonio (2015): "*Delitti contro l'onore*", in Palazzo, Francesco, Paliero, Carlo Enrico (eds.) (2015), p. 143 ss.

Ingrassia, Alex (2012): "*Il ruolo dell'Isp nel ciberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuribili di una responsabilità penale dei* provider *nell'ordinamento italiano*", in Luparia, Luca (eds.) (2012), p. 15 ss., consultabile anche in *Dir. pen. cont.*, 8 novembre 2012.

Ingrassia, Alex (2013): "*La Corte d'Appello assolve i* manager *di* Google *anche dall'accusa di illecito trattamento dei dati personali*", *Dir. pen. cont.* 4 marzo 2013.

Ingrassia, Alex (2014): "*La sentenza della Cassazione sul caso Google*", *Dir. pen. cont.* 6 febbraio 2014.

Ingrassia, Alex (2017): "*Responsabilità penale degli* internet service provider: *attualità e prospettive*", *Dir. pen. proc.*, p. 1621 ss.

Kostoris, Roberto, Viganò, Francesco (2015): *Il nuovo "pacchetto" antiterrorismo*, (Torino, Giappichelli).

La Rosa, Emanuele (2016): "*La protezione dei beni giuridici nel mercato unico digitale tra istanze securitarie e tutela dei diritti*", *Ord. inter. dir. um.*, p. 729 ss.

La Rosa, Mario (2014): "*Tutela della pari dignità: norme antidiscriminazione*", in Pulitanò, Domenico (eds.) (2014), p. 369 ss.

Lobba, Paolo (2011): "*La lotta al razzismo nel diritto penale europeo dopo Lisbona. Osservazioni sulla decisione quadro 2008/913/GAI e sul reato di negazionismo*", *ius17@unibo.it*, 3, p. 109 ss.

Luparia, Luca (2012): "Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*", (Milano, Giuffrè).

Macrillò, Armando (2014): "*Punti fermi della Cassazione sulla responsabilità dell'*"internet provider" *per il reato ex art. 167, d.lgs. n. 163/03*", *Giur. it.*, p. 2016 ss.

Mancuso, Chiara (2009): "*La decisione quadro 2008/913/GAI: due passi in avanti e uno indietro nella lotta europea contro il razzismo*", *Dir. pen. proc.*, p. 645 ss.

Manetti, Michela (2005): "*L'incitamento all'odio razziale tra realizzazione dell'eguaglianza e difesa dello Stato*", in Di Giovine, Alfonso (eds.) (2005), p. 103 ss.

Manna, Adelmo (2001): "*Considerazioni sulla responsabilità penale dell'Isp in tema di pedofilia*", *Dir. info.*, p. 145 ss.

Mannucci Pacini, Ilio (2015): sub *Art. 388 c.p.*, in Dolcini, Emilio, Gatta, Gian Luigi (eds.) (2015), p. 1354 ss.

Marini, Giuliano (1959): "*Condotta e offesa nel delitto di cui all'art. 388 cpv. c.p.*", *Riv. it. dir. proc. pen.*, p. 1218 ss.

Mauri, Roberta Eleonora (2019): "*Applicabile l'art. 57 c.p. al direttore del quotidiano online: un* revirement *giurisprudenziale della Cassazione, di problematica compatibilità con il divieto di analogia*", *Dir. pen. cont.* 28 febbraio 2019.

Melzi d'Eril, Carlo (2016): "*Contrordine compagni: le Sezioni Unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate* on-line *registrate*", *Dir. pen. cont.*, 9 marzo 2016.

Miglio, Mattia (2017): "*I gestori di un sito* internet *rispondono penalmente per i commenti offensivi pubblicati dagli utenti*", *Giurisprudenza penale* web, 1.

Moccia, Sergio (1997): *La perenne emergenza. Tendenze autoritarie nel sistema penale*, (Napoli, Edizioni scientifiche italiane).

Montanari, Matteo (2017): "*La responsabilità delle piattaforme* online *(il caso Rosanna Cantone)"*, *Dir. info*., p. 254 ss.

Moschetta, Teresa Maria (2014): "*La decisione quadro 2008/913/GAI contro il razzismo e la xenofobia: una «occasione persa» per l'Italia?*", in Caggiano, Giandonato (eds.) (2014), p. 781 ss.

Padovani, Tullio (2006): "*Un intervento normativo scoordinato che investe anche i delitti contro lo Stato*", *Guida al dir.*, 14, p. 23 ss.

Palazzo, Francesco, Paliero, Carlo Enrico (2007): *Commentario breve alle leggi penali complementari.* II (Padova, Cedam).

Palazzo, Francesco, Paliero, Carlo Enrico (2015): *Trattato teorico-pratico di diritto penale*, vol. VII, *Reati contro la persona e contro il patrimonio,* a cura di Viganò, Francesco, Piergallini, Carlo, (Torino, Giappichelli).

Panattoni, Beatrice (2018): "*Il sistema di controllo successivo: obbligo di rimozione dell'Isp e meccanismi di* notice and take down", in *Dir. pen. cont.*, 30 maggio 2018.

Pane, Francesca (2015): "*Omofobia e diritto penale: al confine tra libertà di espressione e tutela dei soggetti vulnerabili"*, *Dir. pen. cont*., 24 marzo 2015.

Paoloni, Lucia (2015): "*Le Sezioni Unite si pronunciano per l'applicabilità alle testate telematiche delle garanzie costituzionali sul sequestro della stampa*: ubi commoda, ibi et incommoda?", *Cass. pen.*, p. 3454 ss.

Pavich, Giuseppe, Bonimi, Antonio (2014): "*Reati in tema di discriminazione: il punto sull'evoluzione normativa recente, sui principi e valori in gioco, sulle prospettive legislative e sulla possibilità di interpretare in senso conforme a costituzione la normativa vigente", Dir. pen. cont*., 13 ottobre 2014.

Pazienza, Francesco (1979): *L'inosservanza dei provvedimenti giudiziari*, (Napoli, Jovene).

Pelissero, Marco (2006): "*Osservazioni critiche sulla legge in tema di reati di opinione: occasioni mancate e incoerenze sistematiche (I-II)*", *Dir. pen. proc.*, p. 959 ss.

Pelissero, Marco (2015): "*Omofobia e plausibilità dell'intervento penale"*, *GenIUS*, 1, p. 14 ss.

Petrini, Davide (2004), *La responsabilità penale per i reati via Internet*, (Napoli, Jovene).

Petruso, Rosario (2018): "*Responsabilità delle piattaforme online, oscuramento di siti* web *e libertà di espressione nella giurisprudenza della Corte europea dei diritti dell'uomo*", *Dir. info.*, p. 511 ss.

Picotti, Lorenzo (1999): "*La responsabilità penale dei* service-providers *in internet"*, *Dir. pen. proc.*, p. 501 ss.

Picotti, Lorenzo (2000): voce *Reati informatici*, *Enc. Giur.,* Aggiornamento, VII, (Roma, Treccani), p. 1 ss.

Picotti, Lorenzo (2004): *Il diritto penale dell'informatica nell'epoca di internet*, (Padova, Cedam).

Picotti, Lorenzo (2006): "*Diffusione di idee razziste ed incitamento a commettere atti di discriminazione razziale*", *Giur. merito*, p. 1966 ss.

Picotti, Lorenzo (2006): "*Istigazione e propaganda della discriminazione razziale fra offesa dei diritti fondamentali della persona e libertà di manifestazione del pensiero*", in Riondato, Silvio (eds.) (2006), p. 117 ss.

Picotti, Lorenzo (2007): "*La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in Internet (L. 6 febbraio 2006, n. 38) (parte II)*", *Stud. iur.*, p. 1207 ss.

Piergallini, Carlo (2014): "*Trattamento illecito di dati personali*", *Danno e resp.*, 3, p. 336 ss.

Piffer, Guido (2017): sub *Art. 388 c.p.*, in Forti, Gabrio, Seminara, Sergio, Zuccalà, Giuseppe (eds.) (2017), p. 1224 ss.

Pino, Giorgio (2008): "*Discorso razzista e libertà di manifestazione del pensiero*", *Pol. dir.*, 11, p. 287 ss.

Pugiotto, Andrea (2013): "*Le parole sono pietre? I discorsi d'odio e la libertà di espressione nel diritto costituzionale*", *Dir. pen. cont. – Riv. trim.*, 3, p. 71 ss.

Pugiotto, Andrea (2015): "*Aporie, paradossi ed eterogenesi dei fini nel disegno di legge in materia di contrasto all'omofobia e alla transfobia*", *GenIUS*, 1, p. 6 ss.

Puglisi, Giuseppe (2016): "*A margine della c.d. "aggravante di negazionismo": tra occasioni sprecate e legislazione penale simbolica*", Dir. pen. cont., 15 luglio 2016.

Puglisi, Giuseppe (2018): "*La parola acuminata. Contributo allo studio dei delitti contro l'eguaglianza, tra aporie strutturali e alternative alla pena detentiva*", *Riv. it. dir. proc. pen.*, p. 1325 ss.

Pulitanò, Domenico (2014): *Diritto penale. Parte speciale. Tutela della persona*, vol. I, II ed., (2014) (Torino, Giappichelli).

Pulitanò, Domenico (2015): "*Di fronte al negazionismo e al discorso d'odio*", *Dir. pen. cont.*, 16 marzo 2015.

Riccardi, Giuseppe (2013): "*Omofobia e legge penale. Possibilità e limiti dell'intervento penale*", *Dir. pen. cont. – Riv. trim.*, 3, p. 84 ss.

Riondato, Silvio (2006): *Discriminazione razziale, xenofobia, odio religioso. Diritti fondamentali e tutela penale*, (Padova, Cedam).

Romano, Bartolomeo (2016): *Delitti contro l'amministrazione della giustizia*, VI ed., (Milano, Giuffrè).

Ruggiero, Francescopaolo (2001): "*Individuazione nel ciberspazio del soggetto penalmente responsabile e ruolo dell'*Internet Provider", *Giur. mer.,* p. 586 ss.

Salotto, Francesco (2006): "*Reato di propaganda razziale e modifiche ai reati di opinione (l. 13 ottobre 1975, n. 654; L 24 febbraio 2006, n. 85)*", in Riondato, Silvio (eds.) (2006), p. 167 ss.

Scotto Rosato, Angelo Salvatore (2016): "*Osservazioni critiche sul nuovo "reato" di negazionismo*", *Dir. pen. cont. – Riv. trim.*, 3, p. 280 ss.

Seminara, Sergio (1997): "*La pirateria su internet e il diritto penale*", *Riv. trim. dir. pen. econ.*, p. 96 ss.

Seminara, Sergio (1998): "*La responsabilità penale degli operatori su Internet*", *Dir. info.*, p. 745 ss.

Signorato, Silvio (2015): "*Le misure di contrasto in rete al terrorismo:* black list*, inibizione dell'accesso ai siti, rimozione del contenuto illecito e interdizione dell'accesso al dominio internet*", in Kostoris, Roberto, Viganò, Francesco (eds.) (2015), p. 55 ss.

Spagnoletti, Vittoria (2004): "*La responsabilità dei provider per i contenuti illeciti in Internet*", *Giur. mer*., p. 1922 ss.

Spena, Alessandro (2017): "*La parola (-) odio. Sovraesposizione, criminalizzazione e interpretazione dello* hate speech", *Criminalia – Annuario di scienze penalistiche - 2016,* (Pisa, Edizioni ETS), p. 577 ss.

Stortoni, Luigi (1994): "*Le nuove norme contro l'intolleranza: legge o proclama?*", *Crit. dir.*, p. 14 ss.

Tesauro, Alessandro (2013): *Riflessioni in tema di dignità umana, bilanciamento e propaganda razzista*, (Torino, Giappichelli).

Tesauro, Alessandro (2016): "*La propaganda razzista tra tutela della dignità umana e danno ad altri*", *Riv. it. dir. proc. pen.*, p. 961 ss.

Troper, Michel (1997): "*La legge* Gayssot *e la Costituzione*", *Ragion pratica*, 8, p. 189 ss.

Visconti, Costantino (2006): "*Il legislatore azzeccagarbugli: le "modifiche in materia di reati di opinione" introdotte dalla l. 24 febbraio 2006, n. 85*", *Foro it*.,V, p. 223 ss.

Visconti, Costantino (2008): "*Il reato di propaganda razzista tra dignità umana e libertà di espressione*", in *Ius17@unibo.it*, p. 191 ss.

Visconti, Costantino (2008): *Aspetti penalistici del discorso pubblico*, (Torino, Giappichelli).

Zeno Zencovich, Vincenzo (1998): "*La pretesa estensione alla telematica del regime della stampa. Note critiche*", *Dir. info*., p. 16 ss.

Zeno Zencovich, Vincenzo (2001): "*I "prodotti editoriali" elettronici nella L. 7 marzo 2001, n. 62*", *Dir. info*., p. 153 ss.

Ziccardi, Giovanni (2016): *L'odio* online. *Violenza verbale e ossessioni in rete*, (Milano, Raffaello Cortina Editore).

Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri

Análisis de Big Data y compliance anticorrupción Cuestiones críticas de la práctica actual y escenarios futuros

Big Data Analytics and Anti-corruption Compliance Critical Issues of Current Practice and Future Scenarios

Emanuele Birritteri
Dottorando di ricerca in Diritto e Impresa presso l'Università LUISS "Guido Carli"
ebirritteri@luiss.it

compliance, e-compliance, corruzione, responsabilità da reato degli enti collettivi, pubblica amministrazione

Privacy, *Ne bis in idem*

compliance, e-compliance, corruption, corporate criminal liability, public administration

Abstracts

L'articolo analizza il tema dell'utilizzo di tecniche di *big data analytics* nelle attività di *compliance* anticorruzione nei settori pubblico e privato, evidenziando come tali nuove prassi possano trasformare le caratteristiche attuali della prevenzione del rischio reato nelle organizzazioni complesse. Vengono evidenziati vantaggi e rischi derivanti dall'adozione di questi strumenti informatici, nonché alcuni ipotetici scenari futuri legati alla possibilità di regolamentare in via legislativa l'utilizzo di simili sistemi di *compliance* anche per fini diversi dalla mera gestione del rischio.

El presente artículo analiza la utilización de técnicas de big data en las actividades de compliance anticorrupción en el sector público y privado, evidenciando cómo tales prácticas pueden transformar las características actuales de la prevención del riesgo de delitos en las organizaciones complejas. Se destacan las ventajas y riesgos derivados de la adopción de estos instrumentos informáticos, así como algunos hipotéticos escenarios futuros ligados a la posibilidad de regular por vía legislativa el uso de estos sistemas de compliance, incluso para fines diversos de la mera gestión del riesgo.

This paper addresses the issue of implementation of big data analytics techniques in public and private anti-corruption compliance, highlighting how this new practice can transform the current features of crime-risk prevention activities. The work is aimed at showing the potential benifit and risks related to the adoption of these digital tools, as well as hypothetical future scenarios, including the perspective of regulating the use of such compliance systems also for purposes other than the risk management.

Sommario

1. Nuove tecnologie e contrasto alla corruzione: verso una metamorfosi della *compliance*.

Al giorno d'oggi sia le pubbliche amministrazioni che le imprese private (specie se di notevoli dimensioni) devono fare i conti con una notevole mole di dati eterogenei e prodotti in tempo reale[1]. Tale tipologia di dati (i c.d. *big data*[2]) proprio per queste caratteristiche non possono essere gestiti attraverso le tradizionali metodologie di archiviazione e analisi, ma necessitano inevitabilmente dell'ausilio delle nuove tecnologie[3].

Ben si comprende, quindi, come ciò possa rappresentare un rilevante problema di *governance* per i soggetti coinvolti.

Tuttavia, i recenti sviluppi della prassi in materia dimostrano che esiste la possibilità di trasformare dati asettici in informazioni rilevanti per la prevenzione del rischio corruzione[4].

Insomma, quello che sta iniziando ad emergere in via embrionale è che la gestione dei dati più che rappresentare un problema può in realtà divenire un'interessante opportunità per i settori pubblico e privato, due mondi apparentemente lontani ma che negli ultimi tempi fanno registrare una sempre maggiore osmosi di idee e *best practice* nelle attività di *enforcement* anticorruzione. Osmosi resa possibile anche dall'atteggiamento proattivo di molte realtà imprenditoriali private che, in alcuni casi, hanno sviluppato innovativi meccanismi di prevenzione dei fenomeni corruttivi. E ciò anticipando le stesse scelte di regolazione del legislatore, al di là dell'esistenza di obblighi cogenti[5].

E proprio tale fenomeno si è manifestato con palmare evidenza nell'uso di sistemi di *big data analytics* nell'ambito delle attività di monitoraggio e gestione del rischio corruzione.

Da qualche anno, infatti, specie nel sistema anglosassone si sono implementati strumenti informatici automatizzati di raccolta, confronto e analisi – anche mediante l'uso di algoritmi e *software* di intelligenza artificiale – di una rilevante quantità di dati interni e esterni all'impresa, in particolare in una triplice direzione : 1) identificare indicatori di anomalia e rischio corruzione, nonché ulteriori segnali d'allarme nelle operazioni aziendali (in particolare azioni anomale rispetto ai modelli di comportamento che il sistema qualifica come ricorrenti/ordinari); 2) monitorare il traffico *mail* interno, allo scopo di individuare conversazioni in cui si utilizzino determinate parole chiave considerate "a rischio"; 3) fornire al *management* un *report* in *real-time* in merito a eventuali profili di anomalia (o altri *red flags*) nel comportamento del (o nei dati raccolti sul) *partner*/agente con cui sono in corso determinate operazioni (c.d. *third party due diligence*)[6].

[1] Al riguardo si veda Buttarelli (2017), p. 31 ss.

[2] La letteratura al riguardo è vasta. Per ulteriori approfondimenti sul tema si vedano, senza pretesa di esaustività: Falcone (2017), p. 601 ss.; Zeno-Zencovich (2018), p. 1 ss.; Ponte (2017), p. 31 ss.; Di Porto (2016), p. 5 ss.; Pitruzzella (2016), p. 15 ss.; Ottolia (2017), *passim*; Wachter e Mittelstadt (2019), p. 1 ss.; Levy (2013), p. 73 ss.; Colajanni (2017), p. 79 ss.

[3] Cfr. sul punto il Libro Bianco dell'Agenzia per l'Italia Digitale del marzo 2018, *L'intelligenza artificiale al servizio del cittadino,* p. 52, ove si evidenzia che «…pur rappresentando una miniera di informazioni, i dati hanno bisogno di strumenti adeguati per poter essere sfruttati in tutto il loro potenziale. In particolare, servono modelli e metodi di recupero e filtraggio delle informazioni fondati su tecnologie semantiche e ontologie condivise».

[4] V. anche Hughes Parker (2014), p. 1 ss.

[5] Sul tema specifico della corruzione v.: Severino (2019), p. 1 ss., la quale evidenzia al riguardo che «…una delle sfide già intraprese e che caratterizzeranno gli anni a seguire sarà quella di favorire il più possibile lo scambio di esperienze e buone prassi tra mondo pubblico e privato, dovendosi comprendere come siano esattamente comuni le sfide, le strategie e gli obiettivi da raggiungere per creare un mondo economico veramente competitivo e che sappia affrontare con successo i nuovi rischi della modernità»; Gullo (2017), p. 93 ss.

[6] Va rilevato come il tema al centro della presente analisi, in considerazione della sua novità, non sia ancora stato oggetto di attenzione in letteratura rispetto ai risvolti di carattere penalistico legati all'uso di tali sistemi, avendo piuttosto suscitato l'attenzione dei professionisti operativi della *compliance* rispetto alle potenzialità applicative di questi strumenti. Per una panoramica di tali procedure applicative nella prassi aziendale si vedano, *ex multis*: Olsen *et al.* (2016), p. 1 ss.; Daniels *et al.* (2018), p. 1 ss.
Si veda altresì il rapporto di gennaio 2014 dello *EY Center for Board Matters*, p. 7 ss.: *The bar is raised: anti-corruption compliance now requires big data analytics*. Una ricognizione dei *software* attualmente presenti sul mercato nel settore della c.d. *RegTech*, inoltre, è stata effettuata da *Deloitte*

I *red flag* oggetto di attenzione sono davvero numerosi. Essi vanno, solo per citarne alcuni, dall'identificazione di prezzi d'acquisto, compensi per consulenze e flussi di denaro anomali rispetto alla media dei prezzi di riferimento del settore commerciale e dell'area geografica, all'individuazione di segnali (d'allarme) di possibili conflitti di interesse tra esponenti delle funzioni aziendali coinvolte nelle transazioni e terze parti, fino a movimenti finanziari sospetti rispetto alla "storia" di *business* dell'ente[7].

Si tratta, del resto, di procedure e prassi operative che rappresentano soltanto una parte di un ideale mosaico complessivo la cui immagine ci restituisce chiara l'idea di come ormai il tema dell'intelligenza artificiale abbia fatto ingresso in vari settori del sistema penale: dalla prevenzione pubblica dei reati (c.d. *predictive policing*) attraverso *software* intelligenti in grado di individuare – mediante l'incrocio di svariati dati provenienti dalle fonti più disparate (da documenti di polizia a *social network*) – aree territoriali in cui vi è maggiore probabilità di attività delittuose[8] o di aiutare gli inquirenti a selezionare, tra milioni di file, quelli più "promettenti" per l'indagine[9]; fino all'esercizio della giurisdizione, con l'utilizzo di algoritmi in grado di identificare il rischio di recidiva di determinati soggetti, supportando il giudice nella propria attività di *sentencing*[10].

Le straordinarie potenzialità e la versatilità di questi strumenti hanno fatto sì che fossero utilizzati nelle attività di prevenzione del rischio reato (e in particolare del rischio corruzione) nell'ambito di strutture complesse[11].

Ben poco però si è, sino ad ora, riflettuto sulla possibilità che lo sviluppo di tali procedure possa portare a una vera e propria metamorfosi del volto attuale della *compliance* pubblica e privata: da un sistema che ruota attorno alle classiche attività umane di analisi e indagini preventive "sul campo", a un sistema (parzialmente o integralmente) automatizzato in cui è la sola "macchina" ad assumere su di sé il ruolo di valutare il rischio e di individuare le procedure per gestirlo – e in cui l'uomo svolge soltanto il compito di assicurarsi che il *software* intelligente abbia riserve di "carburante" (cioè dati) sufficienti a poter svolgere i propri adempimenti di sorveglianza.

Si pensi, ad esempio, anche alle prospettive che si stanno aprendo in termini di utilizzo della tecnologia *blockchain* per aumentare la trasparenza e la verificabilità dei dati e dei processi interni alle organizzazioni – con risvolti potenzialmente rivoluzionari anche per il contrasto alla corruzione, ancora del tutto inesplorati[12].

L'obiettivo del lavoro è quindi quello di indagare le potenzialità (e per converso i rischi) legati alla possibile importazione di tali strumenti di *compliance* anticorruzione nella realtà italiana pubblica e privata, delineando, nella parte conclusiva, alcune linee di futuro sviluppo di questi sistemi.

2. *Big Data Analytics* e prevenzione della corruzione nelle pubbliche amministrazioni: quali prospettive?

Prendendo le mosse dalla possibile adozione di questi sistemi in ambito pubblico, e immaginando, in particolare, una loro applicazione nei piani triennali di prevenzione della corruzione delle amministrazioni (nati, come noto, dalla volontà di innervare anche nella P.A.

ed è consultabile al seguente link: https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html#.

[7] Per una panoramica di alcuni di tali *red flags* v.: Berliner e Dupuy (2018), p. 3 ss.; Gee (2015), p. 243 ss.

[8] Sul punto, in particolare, v.: Bonfanti (2018), p. 1 ss.; Kraft (2017), p. 249 ss.

[9] Il riferimento è qui al *software* di intelligenza artificiale denominato RAVN, che ha aiutato il *Serious Fraud Office* britannico a risolvere il noto caso di corruzione c.d. *Rolls-Royce*, strutturando un sistema informatico in grado di indicizzare, sintetizzare e individuare i file più promettenti tra centinaia di migliaia di documenti di rilevanza investigativa, riducendo in modo estremamente significativo il lavoro di analisi degli inquirenti (si veda in particolare un articolo pubblicato al riguardo sul sito del *Financial Times*, www.ft.com, dal titolo: *SFO expected to promote Ravn's crime-solving AI robot*).

[10] Cfr. sul punto, anche per ulteriori approfondimenti: Gialuz (2019), p. 1 ss.; Parodi e Sellaroli (2019), p. 47 ss.

[11] Esistono, peraltro, esempi di applicazione di tali strumenti anche per la prevenzione di illeciti in tema di *market abuse*, nonché in materia ambientale. Per una panoramica al riguardo si vedano: Dombalagian (2016), p. 1 ss.; Glicksman *et al.* (2017), p. 41 ss. Per una compiuta analisi dei legami tra intelligenza artificiale e abusi di mercato v. Consulich (2018), p. 195 ss. Rispetto alle attività della *Securities and Exchange Commission* degli Stati Uniti al riguardo si veda White (2016), p. 1 ss.

[12] V., in particolare, Cariola (2019). Più in generale, per un'analisi delle connessioni tra corruzione, *blockchain* e *bitcoin* v. Kossow *et al.* (2018), p. 1 ss.

l'esperienza dei *compliance program* 231[13]), a nostro avviso un primo problema è quello della qualità e dell'attendibilità dei dati posti al centro dell'analisi informatica[14].

Rispetto a questi modelli, infatti, non esistono *software* dal funzionamento standard, essendo il singolo ente (pubblico o privato) a decidere quali istruzioni dare e quali analisi far svolgere al sistema e, soprattutto, quali dati (interni ed esterni all'ente) far confrontare alla macchina[15].

Un aspetto essenziale delle prassi in esame, infatti, è dato dall'assenza di regolamentazioni pubblicistiche – a livello interno, così come sovranazionale e in seno ad ordinamenti stranieri – sull'utilizzo di queste procedure[16], cosicché ciascuna organizzazione ha assoluta libertà nello strutturare, come meglio crede, siffatti sistemi.

Da qui dunque un primo, delicato, problema che si sta imponendo nei diversi campi di utilizzo dell'AI: la provenienza dei dati da fonti affidabili e sicure. Solo su questo presupposto, infatti, i fattori di rischio che i *big data analytics system* identificano possono essere credibili. È di agevole intuizione, del resto, che usare in questi processi d'analisi l'intera quantità dei dati presenti in Internet rischia di produrre un risultato fuorviante, sicché assicurare una corretta e credibile formazione della base d'indagine appare essenziale (e ciò ovviamente vale anche per le attività private di *compliance*)[17].

Per le amministrazioni pubbliche, peraltro, un simile obiettivo non può dirsi così complesso come all'apparenza potrebbe sembrare. Le nostre amministrazioni, infatti, possiedono uno straordinario patrimonio informativo composto da atti pubblici di varia natura e di intrinseca affidabilità (stante, appunto, la loro natura pubblicistica), nonché diverse banche dati – come, ad esempio, quella degli appalti pubblici – i cui contenuti si rivelano preziosi per individuare possibili *red flag* di interesse per la prevenzione della corruzione[18].

Ciò che spesso manca è appunto la capacità professionale e tecnica di mettere in correlazione tali dati (nonché di stabilire meccanismi di connessione tra le diverse banche dati pubbliche), così pure di processare i loro contenuti; questo è però un problema rispetto al quale tali *software* di *big data analytics* offrono una soluzione[19].

A quel punto, chiaramente, resterebbe il non trascurabile tema di costruire metodologie di indagine informatica il più possibile affidabili, complete e ispirate alle migliori *best practice* nel campo dell'individuazione e della gestione del rischio reato/corruzione[20].

A queste condizioni, ci sembra che l'impiego di tali strumenti nel settore pubblico andrebbe incoraggiato: le pubbliche amministrazioni potrebbero identificare e gestire con maggiore efficienza situazioni di rischio, migliorando i propri piani triennali anticorruzione. Proprio perché, partendo dalla predetta (estremamente affidabile) base di dati, le capacità computazionali del sistema di processare tali informazioni appaiono in grado di identificare il rischio corruzione (in termini di anomalie statistiche e gestionali) in modo estremamente efficace e completo, sottoponendo ad analisi una base di dati e operazioni non analizzabile – per la sua

[13] Sul punto si vedano, per tutti: Severino (2019), p. 1 ss.; Severino (2016a), p. 7, che evidenzia come «…la logica del Piano Nazionale Anticorruzione e poi dei singoli piani anticorruzione delle diverse amministrazioni nonché l'individuazione di un responsabile anticorruzione riflettono da vicino quella dei modelli di organizzazione, gestione e controllo sperimentati nel campo delle persone giuridiche. Si vuole con ciò rafforzare anche nella pubblica amministrazione l'etica della responsabilità e spingere la struttura organizzativa a dotarsi delle cautele e dei presidi necessari a minimizzare il rischio reato. Un percorso nuovo e stimolante che dovrebbe condurre la pubblica amministrazione a essere attrice del processo di prevenzione della corruzione»; Gullo (2018), p. 39, il quale rileva al riguardo che «…la filosofia di fondo è stata quella di coinvolgere i funzionari pubblici in un approccio proattivo alla lotta alla corruzione, costruendo meccanismi di gestione che possano consentire di operare individuando il rischio e predisponendo cautele dirette a minimizzarlo».

[14] Sull'importanza di tali aspetti v., in via generale rispetto ai sistemi giudiziari, anche la *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, elaborata dalla *European Commission for the Efficiency of Justice* (CEPEJ), p. 8 ss.

[15] Sul punto, in particolare, si veda lo studio DGI(2017)12, pubblicato dal Consiglio d'Europa, dal titolo: *Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, p. 6, ove si legge che «…*if further must be considered that designers of algorithmic systems have varying levels of discretion when deciding, for instance, what training data to use or how to respond to false positives, and that the power of the operator of the algorithm may lie in his or her knowledge of the structure of the data set, rather than in insight into the exact workings of the algorithms*».

[16] Sul tema dei legami tra *compliance* e nuove tecnologie e sui problemi connessi alla mancanza di una sufficiente regolazione del settore, si veda, per tutti, Laufer (2017), p. 71 ss.

[17] Più in generale, sul punto, v. la *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, cit., p. 10.

[18] In argomento, in particolare, v. per approfondimenti Falcone (2017), p. 617 ss.

[19] Sul punto, ancora, Falcone (2018), p. 105, il quale peraltro evidenzia come l'organizzazione ragionata e funzionale dei dati sia fondamentale per prevenire la corruzione e in particolare per farlo utilizzando sistemi di *big data analytics*.

[20] A quest'ultimo riguardo, del resto, un grande ausilio è offerto dai diversi strumenti di standardizzazione e supporto alle imprese esistenti in materia di indagini e strutturazione di *compliance program* anticorruzione. Per una panoramica delle *best practice* di costruzione di tali modelli v., in particolare, Giavazzi *et al.* (2014), p. 125 ss.

impressionante mole – nemmeno da un nutrito *team* di esperti[21].

Ciò anche in considerazione della tendenza ad allargare il perimetro della prevenzione amministrativa della corruzione che, come noto, tende ad avere ad oggetto non soltanto l'identificazione di comportamenti di possibile rilevanza penale, ma anche più semplicemente mere ipotesi di *maladministration*. E allora l'identificazione in via informatica di scostamenti dai prezzi standard di settore, eccessi di spesa, anomalie nelle caratteristiche degli appalti e altri *red flags* può diventare un formidabile strumento per eliminare sprechi e combattere inefficienze anche non necessariamente legati a condotte illecite[22].

Certo incentivare (se non addirittura obbligare) le pubbliche amministrazioni a utilizzare questi strumenti ha un costo notevole e rischia di essere controproducente in alcune realtà medio-piccole che già oggi faticano ad essere *compliant* con la normativa nazionale anticorruzione[23].

Al netto però di questo, si dovrebbe riflettere su una regolamentazione ragionata. A quali condizioni, e attraverso quali soluzioni operative, si avrà modo di chiarire non appena soffermeremo la nostra attenzione sul versante delle organizzazioni di matrice privatistica.

Va detto, del resto, che in Italia, da tempo, l'Autorità Nazionale Anticorruzione sta definendo innovative metodologie volte alla costruzione di indicatori di rischio corruzione[24] e, in questa prospettiva, va segnalata la recente adesione dell'ANAC a un contratto quadro per l'implementazione di modelli informatici per l'analisi di *big data*[25].

3. *Big Data Analytics* e *compliance* anticorruzione nel settore privato: categorizzazione e risvolti dogmatico-applicativi delle attuali prassi operative.

Volgendo adesso lo sguardo al settore della *compliance* anticorruzione privata riteniamo che – al di là del già menzionato profilo relativo all'attendibilità dei dati posti alla base dell'analisi – siano identificabili alcuni temi principali.

Innanzi tutto, come visto, dalla prassi sembra emergere come siano le singole società a decidere come strutturare il *software* di analisi, quali dati inserire nel sistema, quali indagini far svolgere alla macchina, in *quali* (e in *quale* segmento temporale delle) procedure aziendali prevederne l'applicazione[26].

Si tratta di procedure polimorfe, in grado cioè di assumere rilievo, a seconda delle tecniche con cui sono costruite e implementate, sia nell'ambito del *risk assessment*, che nell'ambito del *risk management* (come si anticipava, peraltro, ciò può valere *mutatis mutandis* anche laddove si pensi a una applicazione di tali meccanismi nel settore pubblico)[27].

Queste analisi informatiche dei dati, infatti, potranno essere soltanto strumenti di analisi e valutazione (e *non* anche di gestione) del rischio ove l'ente decida di condurle sulla base di una logica *ex post*, sottoponendo cioè semplicemente a revisione il proprio patrimonio infor-

[21] Su tali aspetti v. anche Trapani (2018), p. 10 ss.

[22] Sul tema della *maladministration* v., per tutti, Cantone (2017), p. 4, che evidenzia sul punto l'esistenza di «…un mutamento di prospettiva per cui diventano rilevanti situazioni nelle quali il rischio è meramente potenziale, il conflitto di interessi "apparente", ma in presenza delle quali è necessario entrino in gioco misure di "allontanamento" dal rischio, con scelte che talvolta prescindono completamente dalle condotte individuali».

[23] Non a caso, con la delibera n. 1074 del 21 novembre 2018 l'Autorità Nazionale Anticorruzione ha individuato ulteriori modalità semplificate di applicazione degli obblighi in materia di pubblicità, trasparenza e prevenzione della corruzione per i piccoli comuni – oltre a quelle già identificate nel Piano Nazionale Anticorruzione del 2016 – in attuazione dell'art. 3, comma 1-ter, del d.lgs. n. 33 del 2013 (introdotto dal d.lgs. n. 97 del 2016) in base al quale l'ANAC, con il PNA, può prevedere misure di semplificazione per i comuni con popolazione inferiore ai 15.000 abitanti.

[24] Si veda, in particolare, lo studio pubblicato nel gennaio del 2018 dall'Autorità Nazionale Anticorruzione dal titolo: *Efficienza dei contratti pubblici e sviluppo di indicatori di rischio corruttivo*. Il lavoro è reperibile sul sito dell'Autorità (www.anticorruzione.it).

[25] Cfr. la Determina a contrarre del 5 giugno 2018, a firma del Segretario Generale dell'Autorità, con cui l'ANAC ha disposto l'adesione al contratto quadro Consip per l'affidamento dei Servizi di interoperabilità dati e cooperazione applicativa, finalizzati, tra l'altro, a sviluppare meccanismi per l'integrazione e la gestione di *Big Data*. Il documento è reperibile sul sito dell'Autorità (www.anticorruzione.it).

[26] Cfr. lo studio del Consiglio d'Europa, dal titolo: *Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, cit., p. 6.

[27] Come si rilevava pocanzi, la dottrina non si è ancora occupata di "incasellare" queste prassi nelle categorie generali della disciplina della responsabilità da reato degli enti collettivi. Per una panoramica delle possibilità di utilizzo di questi sistemi, tuttavia, oltre ai contributi pocanzi citati, si veda il rapporto pubblicato dal *Deloitte Center for Regulatory Strategy* (*Americas*) nel 2017, dal titolo: *Compliance modernization is no longer optional. How evolved is your approach?*

mativo (interno ed esterno) per identificare aree sensibili ed esposte al verificarsi di illeciti, senza rendere tali strumenti parte integrante dei singoli protocolli operativi di controllo del rischio reato[28].

In tali casi, invero, l'anomalia documentale verrebbe rilevata in un momento in cui la procedura di formazione della volontà dell'ente si è conclusa. In una fase, quindi, in cui l'eventuale corruzione si è già consumata – con il conseguente radicamento della responsabilità da reato dell'ente.

Ciò non vuol dire che meccanismi così strutturati non abbiano alcuna utilità rispetto alla costruzione dei modelli organizzativi.

Più semplicemente si tratterebbe di tecniche di miglioramento *pro futuro* della *compliance* interna all'organizzazione complessa. Ove, infatti, la base di dati oggetto dell'indagine venga costruita attraverso metodologie credibili – prevedendo l'obbligo di inserire nel sistema IT ogni informazione rilevante e costruendo effettive sanzioni disciplinari nei confronti dei dipendenti per le relative violazioni di tali obblighi di *disclosure* interni – l'attività di *risk assessment* risulterebbe particolarmente valida ed efficace, identificandosi i fattori di rischio non già su valutazioni di massima o controlli a campione, ma sulla base di una ricognizione completa di ogni dato di possibile rilievo e con le straordinarie capacità di calcolo e comparazione di un sistema informatico[29] (in grado di identificare modelli di comportamento anomali e correlazioni tra informazioni non individuabili sulla base della sola valutazione dell'uomo)[30].

Ciò, certamente, potrebbe rappresentare un elemento di rilievo di cui tener conto per valutare le opportune modifiche ai protocolli di gestione del rischio reato e consentirebbe di rafforzare notevolmente la tenuta complessiva del sistema di *compliance*, anche rispetto alla temutissima valutazione del giudice sull'idoneità del modello[31].

Come visto, infatti, in tal caso le esigenze di gestione del rischio non verrebbero rilevate sulla base delle tradizionali attività di indagine empirica gestite da *team* di esperti, ma, al contrario, sulla base di una pervasiva analisi condotta sulla base dell'intero patrimonio informativo rilevante dell'organizzazione complessa di riferimento e con metodologie di analisi di dati in grado di individuare profili di criticità a volte (se non sempre) non identificabili altrimenti[32].

Tali meccanismi, peraltro, consentono di allocare efficacemente i costi della *compliance* verso i settori di attività dell'ente che più necessitano di attenzione in tal senso, evitando lo spreco di risorse[33].

Ma, spingendoci oltre, va rilevato come le società potrebbero decidere di compiere un passo ulteriore, prevedendo l'applicazione di tali strumenti non soltanto nella direzione appena indicata, ma anche nei singoli protocolli operativi di gestione del rischio corruzione[34], facendo riferimento nel modello organizzativo all'utilizzo di questi meccanismi di *risk detecting* nelle proprie operazioni quotidiane.

Ciò, nella prassi, accade principalmente rispetto alle procedure di c.d. *due diligence* nei confronti di terze parti, ove ogni procedura decisionale in merito all'opportunità di intraprendere un determinato affare è anticipata dalle predette attività di *data analytics*, con la previsione di un *report in real time* al *management* in merito alle eventuali anomalie rilevate e ai conseguenti rischi legali e di non conformità connessi ai possibili rapporti da intraprendere con il singolo

[28] In argomento v. anche Pitaro (2018), p. 1 ss.

[29] Sul tema, in generale, della rilevanza giuridico-penale dell'automazione quale strumento di sostituzione dell'attività dell'uomo v., per tutti, Picotti (2019), p. 43 ss., secondo il quale al riguardo occorre muovere dalla premessa che la specifica qualità tecnica dell'informatica che interesse il penalista è costituita «…dall'*automazione* dei trattamenti o processi di elaborazione dei dati, secondo *programmi* specifici, che consentono di pervenire, con l'esecuzione di appositi ed evoluti algoritmi, a risultati *complessi* e straordinariamente più *precisi*, in tempi infinitamente più *rapidi* rispetto a quelli conseguibili con l'attività dell'uomo in carne ed ossa». Per una visione critica sull'automazione nel settore legale v. Pasquale (2019), p. 1 ss.

[30] In generale, sul tema della costruzione di un *fraud data analytics plan* nell'ambito del contrasto alla corruzione v. Vona (2017), p. 269 ss. (e, con riferimento specifico al settore del *procurement*, p. 247 ss.). In argomento v. anche Zwiebel (2017), p. 1 ss.

[31] Su tale aspetto v., per tutti: Severino (2016b), p. 76, la quale evidenzia al riguardo che «…in assenza di indicazioni vincolanti e specifiche, la valutazione di idoneità del modello è interamente rimessa alla discrezionalità del giudice, alla sua sensibilità e conoscenza dei meccanismi aziendali ed economici, alla corretta applicazione di quel complesso e delicato giudizio (*ex post*) che riguarda la tenuta (*ex ante*) del modello. In tale contesto appare evidente che senza un impegno da parte del legislatore non sembra facile assicurare la necessaria uniformità applicativa in materia e il saldo ancoraggio del modello alla sua vocazione «premiale», al riparo il più possibile dal rischio di sconfinamenti nella logica del «senno di poi» - che vede la verificazione del reato come una spia dell'inidoneità del modello, in particolar modo quando a venire in gioco è l'agire dei soggetti apicali»; Manacorda (2017), p. 71 ss.

[32] Sul tema, in generale, dell'importanza del *risk assessment* nella costruzione dei modelli organizzativi v. Piergallini (2013), p. 843.

[33] Cfr., in particolare, il rapporto pubblicato da *Deloitte* dal titolo: *Compliance modernization is no longer optional. How evolved is your approach?*, cit., p. 5.

[34] Sulla costruzione dei protocolli di gestione v. per tutti, ancora, Piergallini (2013), cit., p. 845 ss.

partner/agente commerciale (specie per affari all'estero rispetto ai quali può esistere un rischio di corruzione internazionale)[35].

In tali casi, l'attività di *big data analytics* diventa un vero e proprio strumento concreto di prevenzione, innervato nei protocolli di controllo del rischio reato.

Una simile procedimentalizzazione delle attività, peraltro, se correttamente strutturata ponendo attenzione agli aspetti critici sopra segnalati in termini di affidabilità e completezza dei dati oggetto di analisi, potrebbe ritenersi un utile strumento per costruire un meccanismo di prevenzione tale da non poter essere eluso se non ricorrendo a condotte fraudolente e di notevole complessità tecnica (alla luce della peculiare diffusione del controllo su ogni dato aziendale e della necessità di aggirare un sistema informatico molto articolato e protetto da sofisticate misure di sicurezza)[36]. Così rafforzandosi notevolmente l'apparato di *compliance* della persona giuridica in relazione all'*enforcement* del d.lgs. n. 231 del 2001.

Non mancano, tuttavia, le ombre nello scenario sin qui delineato.

Adottare il predetto strumento di *report in real time* al *management*, infatti, se da un lato rafforza l'idoneità preventiva (astratta) del *compliance program*, dall'altro si espone a facili censure di non efficace attuazione del modello (chiaramente allorquando il pericolo segnalato sia ignorato dagli organi aziendali). Un profilo, quest'ultimo, su cui come noto molto spesso si appuntano le decisioni che negano l'efficace esimente del modello nei procedimenti per responsabilità da reato delle persone giuridiche[37].

Ancora, in termini più generali si è rilevato come l'automazione della *compliance* potrebbe dar luogo ad una modifica della base fattuale (umana e non anche o solo tecnologica) su cui oggi si basa la responsabilità da reato degli enti collettivi, ponendo non indifferenti problemi rispetto alla possibilità di ritenere sussistente la colpa in organizzazione della persona giuridica – specie allorquando la commissione dell'illecito penale sia stata resa possibile da un difetto di progettazione del sistema informatico di prevenzione che l'ente si limita ad utilizzare, senza esserne l'autore[38].

L'effettiva messa in atto di alcune di queste pratiche di sorveglianza generalizzata apre poi l'ulteriore profilo – che qui può essere solo accennato – dell'eventuale ammissibilità di simile procedure rispetto alla disciplina dei controlli sui lavoratori[39], nonché in tema di tutela della *privacy* e del c.d. domicilio informatico del dipendente: basti pensare, a quest'ultimo riguardo, al consolidato orientamento della giurisprudenza della Corte di Cassazione in termini di configurabilità del reato di accesso abusivo a sistema informatico nel caso di controllo delle *mail* dei dipendenti (pubblici o privati)[40].

L'implementazione di queste procedure, peraltro, può sollevare a volte il tema della legittimità del trattamento dei dati personali dei soggetti coinvolti dalle indagini informatiche[41],

[35] Uno dei software più diffusi al riguardo sul mercato, in particolare, è il sistema CERICO, oggi offerto da *Dow Jones Risk & Compliance* (www.dowjones.com), che effettua una valutazione su svariati dati, alcuni dei quali offerti direttamente dall'agente di cui deve valutarsi l'affidabilità, assegnando in *real time* un determinato tasso di rischio all'operazione commerciale e consentendo così al *management* di decidere se intraprendere o meno l'affare. Un altro sistema molto diffuso è il software WORLD CHECK della *Thomson-Reuters* (www.risk.thomsonreuters.com/products/world-check), che compara dati – correggendo anche tutti i possibili falsi positivi – provenienti da svariati fonti pubbliche (come giornali e media in generale, tribunali, siti web governativi) al fine di valutare i rischi legali e reputazionali che l'impresa può correre intraprendendo una certa operazione, anche affidandosi a determinati agenti. Si analizzi anche, al riguardo, l'*Enterprise Legal Risk Management Framework*, su cui v. Apollon (2017), p. 486 ss.

[36] Sul tema dell'elusione fraudolenta si veda, per tutti, il lavoro monografico di Tripodi (2013), *passim*.

[37] Cfr., in particolare, Manacorda (2017), cit., p. 68, il quale rileva che, riferendosi al tema dell'efficace attuazione, il legislatore «…ha inteso rimarcare che l'onere di auto-organizzazione in chiave prevenzionistica non deve rimanere meramente cartolare, negando la valenza esimente ad un modello che, per quanto adottato correttamente, non sia ritenuto essere sorretto da impegni, procedure e sforzi adeguati. Si tratta di un'esigenza più che comprensibile, la quale introduce tuttavia un elemento valutativo (ulteriormente) incerto in sede di apprezzamento ad opera del giudicante, e sul quale – non a caso – tendono ad appuntarsi le pronunce giudiziarie».

[38] Così, in particolare, Selvaggi (2019), p. 7 ss. del dattiloscritto, il quale tuttavia rileva che, per evitare un arretramento rispetto agli attuali sviluppi della colpa di organizzazione, difficilmente potrebbe prescindersi «…dalla verifica di un contributo specifico dell'ente diverso da quello o da quelli che abbiano confezionato la tecnologia applicata alla compliance», dovendosi in particolare esaminare «…i comportamenti tenuti da coloro, diversi dall'autore del reato, che abbiano operato lungo le filiere della decisione e del controllo […] dal momento genetico della installazione dei sistemi all'interno della compagine organizzativa e del loro eventuale adattamento al mancato intervento correttivo […] che le circostanze concrete eventualmente richiedano». Sul tema, in generale, della colpa di organizzazione v., per tutti, Paliero, Piergallini (2006), p. 167 ss.

[39] Per approfondimenti al riguardo si vedano, in particolare: Proja (2016), p. 547 ss.; Tebano (2017), p. 3 ss.

[40] In argomento v., *ex multis*: Cass., Sez. V, 31 marzo 2016, con nota di Colucci (2016), p. 32 ss. Cass., Sez. VI, 14 dicembre 1999, con nota di Cuomo (2000), p. 2990 ss.

[41] In alcune ipotesi, infatti, in caso di controllo delle mail dei dipendenti o analisi di determinati documenti di rilievo non solo aziendale, tali procedure potrebbero qualificarsi come pratiche di trattamento dei dati personali, con tutto ciò che ne deriva in termini di ulteriori problematiche e adempimenti di *compliance* normativa per le organizzazioni complesse coinvolte. Per ulteriori approfondimenti v., in particolare, Lynskey (2019), p. 162 ss.

anche in considerazione del fatto che l'art. 22 del Regolamento europeo sulla protezione dei dati personali[42] – nonché l'art. 11 della Direttiva 2016/680/UE sulla protezione dei dati personali nell'attività di prevenzione, indagine, accertamento e perseguimento di reati – vietano le decisioni basate unicamente su trattamenti automatizzati e stabiliscono il diritto dell'interessato di ottenere l'intervento umano nel procedimento di formazione di volontà da parte del titolare del trattamento[43].

Si tratta di una questione per certi versi già sperimentata con riferimento all'utilizzo di algoritmi intelligenti nelle c.d. attività di *sentencing* da parte del giudice, sollevandosi in tal caso il tema dell'assenza di possibilità concrete di difesa da parte del condannato rispetto alla contestazione di una valutazione compiuta interamente da una macchina, senza alcun intervento di mediazione da parte dell'uomo[44].

Una problematica, quest'ultima, che potrebbe a ben vedere verificarsi anche con riferimento all'utilizzo dei predetti sistemi di *data analytics* nell'ambito delle attività di *compliance*.

Infatti, l'*output* prodotto dai *software* in parola non soltanto potrebbe basarsi su un trattamento di dati (a volte, personali) integralmente automatizzato e senza alcun intervento umano di "mediazione valutativa" del risultato dell'analisi, ma potrebbe determinare, con tutto ciò che ovviamente ne consegue, la scoperta di elementi fattuali indizianti a carico di (o l'assunzione di decisioni disciplinari o di altra natura in vario modo impattanti su) diversi dipendenti o altri soggetti coinvolti nell'analisi informatica.

Non a caso, pertanto, le predette normative eurounitarie prevedono la necessità che il risultato di decisioni – connesse al trattamento di dati – che producono effetti giuridici o incidono significativamente sulla vita dell'interessato non possa basarsi sul solo prodotto del trattamento automatizzato, ma come quest'ultimo debba costituire in sostanza un elemento oggetto di una più ampia considerazione da parte del responsabile del trattamento (con un correlato diritto di pretendere un simile intervento "umano" da parte dell'individuo coinvolto)[45].

Peraltro, la possibilità concreta che attraverso l'uso della *big data analytics* possano individuarsi elementi indizianti a carico di persone fisiche solleva l'ulteriore problematica delle connessioni che possono istaurarsi tra queste procedure di *compliance* e le *corporate internal investigation*, anche perché le pratiche in analisi potrebbero esse stesse diventare uno degli strumenti attraverso cui l'ente può svolgere le proprie indagini interne[46]. E ciò, chiaramente, impone di individuare il sistema di garanzie da riconoscere ai soggetti coinvolti, specie in considerazione del fatto che – fatte salve le ipotesi in cui tali investigazioni possano qualificarsi come indagini difensive ai sensi degli artt. 391-*bis* ss. del codice di rito – il nostro apparato di regolazione non appare privo di lacune sotto tali profili[47].

Senza contare, poi, come si anticipava, le difficoltà connesse alle (limitate) possibilità di contestare il risultato cui il sistema informatizzato sia pervenuto in considerazione della complessità di comprendere le modalità (spesso oscure) attraverso cui la macchina ha optato per una determinata soluzione valutativa[48].

[42] Cfr. Regolamento 2016/679/UE relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati.

[43] In argomento, di recente, anche per una più ampia disamina del tema della tutela penale dei dati personali, v. D'Agostino (2019), p. 17 ss.

[44] Per approfondimenti sul tema dell'*evidence-based sentencing*, oltre ai contributi pocanzi citati, si veda anche Starr (2014), p. 803 ss.

[45] Sul punto Gialuz (2019), cit., p. 17, il quale rileva peraltro a tale riguardo come «…accanto all'obbligo di un intervento umano andrebbe ritenuta sussistente quella che, nel lessico processualpenalistico, chiameremmo regola di valutazione, in forza della quale l'*output* prodotto dall'IA va considerato come un mero indizio, che va sempre corroborato con altri elementi di prova». Per un approfondimento sugli aspetti di interesse penalistico della direttiva 2016/680/UE v. anche Flor (2019), p. 134 ss.

[46] Sul tema delle *internal investigation* v., in particolare, Mancuso (2016), p. 217 ss.; Bourtin *et al.* (2016), p. 199 ss. Nella lettura internazionale v., per tutti, Nieto (2014), p. 69 ss.

[47] Al riguardo, in particolare, anche per un'analisi delle prospettive *de iure condendo* v. Nicolicchia (2014), p. 805 ss., il quale evidenzia come «…ove non fosse possibile inquadrare le investigazioni interne poste in essere dal soggetto collettivo nei canoni di una indagine difensiva compiuta ai sensi degli artt. 391 *bis* e ss. c.p.p., ci si troverebbe di fronte ad un'attività incidente sui diritti dell'indagato per il reato presupposto e potenzialmente assai pregiudizievole per la sua sorte processuale, la quale risulterebbe però sprovvista di qualsivoglia specifica regolamentazione. L'eventualità segnalata appare tutt'altro che inverosimile, basti pensare, in via di prima approssimazione, al compimento di attività di indagine da parte di soggetti non investiti dell'apposito incarico professionale risultate da atto scritto ai sensi dell'art. 327 *bis* c.p.p., o addirittura sprovvisti della stessa qualifica di avvocato, ipotesi assai verosimile nei processi di *internal audit*, dove diverse specializzazioni e competenze vengono in rilievo».

[48] Sul problema della trasparenza e dell'intellegibilità dei sistemi di *algorithmic decision-making* v., in particolare, Chiao (2019), p. 135. In argomento, però, va segnalato che la *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, elaborata dalla *European Commission for the Efficiency of Justice* (CEPEJ), p. 55, evidenzia, per quanto avuto riguardo al contesto specifico del processo penale, che «*..the party concerned should have access to and be able to challenge the scientific validity of an algorithm, the weighting given to its various elements and any erroneous conclusions it comes to whenever a judge suggests that he/she might use it before making his/her decision*». V. al riguardo anche Gialuz (2019), cit., p. 13.

Insomma, a fronte degli indubbi vantaggi che, come visto, l'implementazione di questi sistemi potrebbe determinare nel rafforzare il sistema di *compliance* anticorruzione delle persone giuridiche, l'utilizzo di tali *software* espone oggi l'impresa a rischi legali su versanti diversi, ma non meno delicati, e per la cui gestione è indispensabile un approccio multidisciplinare.

Laddove, quindi, lo svolgimento di simili attività di *compliance* dovesse trovare in futuro sempre maggiore riscontro nella prassi, non potrà che essere il legislatore a farsi carico di regolare la materia, bilanciando correttamente i diversi interessi in gioco.

Non si può, del resto, "scaricare" sul privato un compito tipicamente pubblicistico come quello di prevenire reati e fenomeni illeciti senza fornire a tali soggetti adeguati strumenti (anche normativi) per svolgere tale ruolo e anzi sanzionando gli enti che si avvalgono di innovative metodologie di gestione del rischio[49].

Vediamo adesso di analizzare quali potrebbero essere alcune delle (possibili) strade da percorrere nella direzione di una (ipotetica) regolazione del settore in futuro.

4. (Ipotetici) scenari futuri tra positivizzazione legislativa delle cautele anticorruzione e premialità per gli enti virtuosi: alcuni spunti.

Lo sforzo che si è sin qui compiuto è stato quello di illustrare il funzionamento degli strumenti di *data analytics* nel settore della compliance (anzitutto anticorruzione) nei settori pubblico e privato e di mettere in risalto alcuni punti di frizione con diritti fondamentali del singolo.

Si tratta di un orizzonte che, a prima vista, sembra ancora lontano, riservato a strutture organizzative complesse all'avanguardia, e destinato solo in futuro ad assumere contorni più precisi.

La rapida evoluzione della tecnologia e la sua costante diffusione ci dicono tuttavia che, prendendo a prestito le oramai celebri considerazioni del Presidente della Corte Suprema degli Stati Uniti *Roberts*, il futuro è già tra di noi[50]. L'insegnamento che proviene, come visto, dall'utilizzo degli algoritmi predittivi, in chiave di prevenzione della criminalità e in fase di decisione giudiziale sul *quantum* di pena, è davvero eloquente.

Quell'esperienza deve essere da monito anche per gli altri settori in cui oggi si affaccia il tema dell'impiego dell'AI per individuare fonti di rischio-reato e progettare idonee misure preventive.

Se, come appare verosimile, si diffonderanno gli analizzati sistemi di analisi di quantità enormi di dati, si porrà l'esigenza di approntare, sulla scia magari di una regolamentazione del fenomeno nell'ambito pubblico, una disciplina anche nel settore privato. Quali dunque le linee portanti di siffatta disciplina?

Qui ci sembra che possa essere di aiuto il dibattito maturato rispetto alla possibile riforma del d.lgs. n. 231 del 2001 circa la necessità di procedere a una positivizzazione dall'alto delle cautele di cui richiedere l'adozione agli enti collettivi[51]. In questa prospettiva potrebbe infatti trovare spazio anche una presa di posizione legislativa in merito all'individuazione di uno *standard* minimo delle tecniche di costruzione e utilizzo di questi sistemi (in particolare con riferimento a uno dei principali problemi emergenti dalle esaminate prassi, ovverosia quello dell'individuazione della base di dati da analizzare, della loro fonte nonché delle tipologie di

[49] Nell'ambito della letteratura internazionale sulla responsabilità da reato degli enti collettivi, per un'analisi di tali problematiche nell'ambito della "*partnership*" pubblico-privato per contrastare i *corporate crimes* – in particolare nel senso di una non corretta distribuzione delle responsabilità di *enforcement* tra regolatore e soggetti regolati – v., per tutti, Laufer (2018), p. 392 ss. Nella dottrina italiana v., invece, Centonze (2017), p. 945 ss.

[50] L'affermazione è stata ripresa di recente da Gialuz (2019), cit., p. 1, il quale ricorda che «…due anni fa, durante un incontro pubblico, venne chiesto al Presidente della Corte suprema degli Stati Uniti, John Roberts, se potesse prevedere il giorno in cui le *smart machines*, guidate da intelligenze artificiali, potranno assistere il giudice nella ricostruzione del fatto o addirittura intervenire nel processo di *decision-making*. La risposta del giudice Roberts è stata più sorprendente della domanda: "*It's a day that's here*" ha detto, "*and it's putting a significant strain on how the judiciary goes about doing things*"».

[51] In tale direzione v., *ex multis*, anche per ulteriori riferimenti bibliografici: Piergallini (2013), cit. p. 860 ss.; Manes, Tripodi (2016), p. 137 ss.; Manacorda (2017), cit., p. 111, il quale peraltro rileva che «…il terreno che ci sembra si presti meglio ad un esercizio di tal fatta è tuttavia quello della corruzione, ove si coagulano una molteplicità di elementi di segno convergente». In argomento si vedano anche i rilievi critici di Mongillo (2011), p. 82. Per un'analisi delle ulteriori posizioni emerse in dottrina sul tema si rinvia, anche per gli opportuni riferimenti bibliografici, a Colacurci (2016), p. 77 ss.

indagini da compiere).

Infatti, uno degli aspetti più delicati emerso dalla dinamica applicativa del d.lgs. n. 231 del 2001 è legato, come noto, alla pressoché totale assenza di decisioni che riconoscano l'idoneità preventiva dei modelli organizzativi, tenuto conto del fatto che il legislatore non fornisce alle imprese nient'altro che indicazioni di massima sull'ossatura del *compliance program*[52].

Da qui la proposta, appena richiamata, di positivizzare per settori differenziati le cautele da imporre all'ente, stabilendo una presunzione di idoneità relativa del modello organizzativo conforme alle indicazioni legislative[53].

Nella materia anticorruzione, quindi, l'implementazione di queste procedure di *big data analytics* potrebbe costituire una delle indicazioni da fornire all'ente in merito alle cautele da implementare per costruire il proprio sistema di *compliance*.

Ciò, ovviamente, a patto che il legislatore – è utile ribadirlo – chiarisca esattamente e nel modo più preciso possibile le fonti di dati da analizzare, le indagini da far compiere al sistema e le metodologie di analisi.

Una soluzione equilibrata potrebbe peraltro essere quella di prevedere un'ulteriore cautela per l'impresa consistente nella registrazione di ogni transazione aziendale di rilievo, istituendo un apposito sistema di controllo interno per verificare che ogni operazione di disposizione di *asset* aziendali si svolga nel rispetto delle *policy* di prevenzione del *management* dell'impresa, e ciò anche al fine di rafforzare la completezza e l'affidabilità della base di dati da sottoporre a indagine informatica.

Si tratterebbe, del resto, di una scelta di regolazione non sconosciuta ad altri ordinamenti, seppur nella differente ottica dell'istituzione di un vero e proprio obbligo legale: negli Stati Uniti, ad esempio, le *accounting provisions* del *Foreign Corrupt Practices Act* prevedono per l'appunto obblighi di registrazione di tal fatta e l'implementazione di un connesso sistema di controllo interno (presidiati, peraltro, da rigorose sanzioni penali e civili capaci di estendersi a certe condizioni anche alla *holding* per violazioni commesse nell'ambito di altre *firms* del gruppo) a carico di alcune società emittenti strumenti finanziari negli USA[54].

Un altro tema, infine, potrebbe essere quello di sfruttare il patrimonio informativo prodotto dai *software* di analisi per procedure di *self reporting* alle autorità pubbliche[55]. Procedure cui eventualmente collegare benefici di intensità graduabile: dalla riduzione del carico sanzionatorio alla radicale non punibilità per l'ente che si autodenunci[56].

Il legislatore, infatti, potrebbe ritenere che il rischio evidenziato, in relazione a tali procedure, di una strumentalizzazione dell'autodenuncia (in termini di selezione opportunistica dei dati interni da diffondere[57]) possa essere superato affidando interamente al sistema informatico il compito di individuare gli elementi alla base della *disclosure*, eliminando il filtro dell'uomo e costruendo il *software* in modo tale che non possa essere artificiosamente modificato.

Non ci nascondiamo peraltro come quest'ultima prospettiva non sia di facile realizzazione e rischi di creare molti più problemi di quanti in realtà ne possa risolvere.

Quel che è certo, tuttavia, è che in un modo o nell'altro il tema della premialità per gli enti virtuosi, che impiegano con spirito proattivo ingenti risorse nelle loro attività di *compliance*, dovrà essere affrontato. Il sistema, insomma, prima o poi dovrà fare i conti con sé stesso, offrendo alle imprese un quadro di regolazione moderno per implementare le attività di prevenzione del rischio reato, ma stabilendo al contempo meccanismi e regole di compor-

[52] Su tali aspetti v., per tutti, Severino (2016b), cit., p. 74 ss.

[53] In tale direzione, in particolare, Manes, Tripodi (2016), cit., p. 168.

[54] Si tratta, in particolare, di disposizioni autonome dalle *antibribery provisions* dell'FCPA, e per la mera violazione delle quali l'ente viene sanzionato anche allorquando non si sia verificata alcuna vicenda corruttiva. Per approfondimenti v., *ex multis*: Vuona (2019), p. 979 ss.; Woody (2017), p. 101 ss.; Jordan (2017), p. 1 ss. Un aspetto di ulteriore rilievo, inoltre, è dato dal fatto che l'adozione dell'*anticorruption compliance program* rappresenta un aspetto essenziale del sistema di controllo interno descritto dalle *accounting provisions* dell'FCPA: sul punto, in particolare, si veda Deming (2012), p. 118.

[55] Nella letteratura internazionale sul tema v., per tutti, in particolare rispetto alla valorizzazione del *self-reporting* per l'accesso a procedure negoziate di definizione dei procedimenti a carico dell'ente (in particolare DPAs e NPAs): Arlen (2017), p. 1 ss. Sul tema v. anche Fiorella, Selvaggi (2018), p. 121 ss.

[56] Per una proposta in tale ultima direzione nella dottrina italiana v., in particolare, Centonze (2017), cit., p. 986, il quale in particolare propone l'introduzione, nella trama del d.lgs. n. 231 del 2001, di un nuovo art. 17-*bis* (rubricato: Causa di esclusione della responsabilità), che, si spiega, «…potrebbe dunque suonare così: 1. *Quando il reato è stato commesso dalle persone indicate nell'art. 5, comma 1, l'ente non risponde se prima della notifica dell'informazione di garanzia, in relazione al predetto reato, abbia fornito all'autorità di polizia o all'autorità giudiziaria elementi di prova determinanti per l'esatta ricostruzione del fatto e per l'individuazione degli autori. 2. In ogni caso, l'esclusione della responsabilità è subordinata alla riparazione delle conseguenze dell'illecito ai senti dell'art. 17. 3. È comunque disposta la confisca del profitto che l'ente ha tratto dal reato, anche nella forma per equivalente*».

[57] Per alcuni rilievi critici al riguardo v., in particolare, Mongillo (2018), p. 380 ss.

tamento chiari, osservati i quali l'ente possa nutrire la ragionevole aspettativa di andare esente da responsabilità[58].

Bibliografia

Apollon, Garrick (2017): "FCPA compliance should not cost «an arm and a leg»: assessing the potential for enhanced cost-efficiency and effectiveness for an anti-corruption compliance program with the implementation of an enterprise legal risk management framework", *Penn State Journal of Law & International Affairs*, vol. 5, n. 2, pp. 486-537.

Arlen, Jennifer (2017): "Corporate Criminal Enforcement in the United States: Using Negotiated Settlements to Turn Corporate Criminals Into Corporate Cops", *NYU School of Law Public Law Research Paper n. 17.12*, april 1, 2017.

Berliner, Daniel, Dupuy, Kendra (2018): "The promise and perils of data for anti-corruption efforts in international development work", U4 Brief 2018:7, Michelsen Institute (www.u4.no).

Bonfanti, Angelica (2018): "*Big data* e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali", *La rivista di diritto dei media*, 3, pp. 1-13.

Bourtin, Nicolas, Houle, Amanda (2016): "Investigazioni interne: uno sguardo all'esperienza americana", in Centonze Francesco, Mantovani Massimo (eds.): "La responsabilità «penale» degli enti. Dieci proposte di riforma" (Bologna, il Mulino), pp. 199-215.

Buttarelli, Giovanni (2017): "Le sfide dei Big Data tra evoluzione tecnologica, etica e interessi collettivi", *Gnosis*, 2, pp. 31-39.

Cantone, Raffaele (2017): "Il sistema della prevenzione della corruzione in Italia", *Diritto penale contemporaneo*, 27 novembre 2017.

Cariola, Gianfranco (2019): "Così la blockchain aggiorna i controlli interni", *Quotidiano del Fisco* (il Sole24ore), 16 febbraio 2019.

Centonze, Francesco (2017): "Responsabilità da reato degli enti e *agency problems*", *Rivista italiana di diritto e procedura penale*, III, pp. 945-987.

Chiao, Vincent (2019): "Fairness, accountability and transparency: notes on algorithmic decision-making in criminal justice", *International Journal of Law in Context*, 15, pp. 126-139.

Colacurci, Marco (2016): "L'idoneità del modello nel sistema 231, tra difficoltà operative e possibili correttivi", *Diritto penale contemporaneo – Rivista trimestrale*, 2, pp. 66-79.

Colajanni, Michele (2017): "Il ruolo del *big data analytics* e *machine learning* nella sicurezza", *Gnosis*, 2, pp. 79-89.

Colucci, Giuseppe (2016): "L'accesso abusivo all'e-mail del dipendente protetta da password", *Guida al Lavoro*, 20, pp. 32-37.

Consulich, Federico (2018): "Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato", *Banca, borsa e titoli di credito*, 2, pp. 195-234.

Cuomo, Luigi (2000): "La tutela penale del domicilio informatico", *Cassazione penale*, 11, pp. 2990-3002.

[58] Sul tema del rafforzamento delle logiche premiali del d.lgs. n. 231 del 2001, v., per tutti, Severino (2018), p. 1101 ss.

D'Agostino, Luca (2019): "La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al d.lgs. 10 agosto 2018, n. 101", *Archivio penale*, 1, pp. 1-58.

Daniels, Donna *et al.* (2018): "Real Risks, Artificial Intelligence: The Next Wave of Anti-Corruption Compliance?", *The Anti-corruption Report* (www.anti-corruption.com), v. 7, n. 4, february 2018.

Deming, Stuart H. (2012): "Internal Controls and Anti-Bribery Compliance", *The Global Business Law Review*, vol. 3:1, pp. 103-141.

Di Porto, Fabiana (2016): "La rivoluzione "big data". Un'introduzione", *Concorrenza e mercato*, 1, pp. 5-14.

Dombalagian, Onnig H. (2016): "Preserving Human Agency in Automated Human Compliance", *Brooklyn Journal of Corporate, Financial & Commercial Law*, WP n. 16-11, pp. 1-40.

Falcone, Matteo (2017): "Big Data e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica", *Rivista trimestrale di diritto pubblico*, 3, pp. 601-639.

Falcone, Matteo (2018): "La *big data analytics* per conoscere, misurare e prevenire la corruzione", in Gnaldi Michela, Ponti Benedetto (eds.): "Misurare la corruzione oggi" (Milano, Franco Angeli), pp. 90-110.

Fiorella, Antonio, Selvaggi, Nicola (2018): "Dall'«utile» al «giusto». Il futuro dell'illecito dell'ente nello 'spazio globale'" (Torino, Giappichelli).

Flor, Roberto (2019): "*Cyber-criminality*: le fonti internazionali ed europee", in Cadoppi Alberto, Canestrari Stefano, Manna Adelmo, Papa Michele (eds.): "Cybercrime" (Utet, Torino), pp. 35-96.

Gee, Sunder (2015): "Fraud and Fraud Detection: A Data Analytics Approach" (Hoboken, John Wiley & Sons).

Gialuz, Mitja (2019): "Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei *risk assessment tools* tra Stati Uniti ed Europa", *Diritto penale contemporaneo*, 29 maggio 2019.

Giavazzi, Stefania *et al.* (2014): "The ABC Program: An Anti-Bribery Compliance Program Recommended to Corporations Operating in a Multinational Environment", in Manacorda Stefano, Centonze Francesco, Forti Gabrio (eds.): "Preventing Corporate Corruption. The Anti-Bribery Compliance Model" (Londra, Springer), pp. 125-177.

Glicksman, Robert L., Markell, David L., Monteleoni, Claire (2017): "Technological Innovation, Data Analytics and Environmental Enforcement", *Ecology Law Quarterly*, 44:41, pp. 41-88.

Gullo, Antonio (2017): "Il contrasto alla corruzione tra responsabilità della persona fisica e responsabilità dell'ente: brevi note", in Castaldo Andrea R. (editor): "Il Patto per la legalità. Politiche di sicurezza e di integrazione" (Milanofiori Assago, Wolters Kluwer), pp. 89-99.

Gullo, Antonio (2018): "Note minime sul rapporto tra diritto amministrativo e diritto penale", *Luiss Law Review*, 2, pp. 35-41.

Hughes Parker, Rebecca (2014): "Ernst & Young Experts Reveal How Forensic Data Analytics Can Transform Anti-Corruption Compliance", *The Anti-corruption Report* (www.anti-corruption.com), v. 3, n. 9, April 2014.

Jordan, Jon (2017): "BNY Mellon and Qualcom: a recent focus on improper hiring practices in violation of the Foreign Corrupt Practices Act", *Loyola Law Review*, vol. 63, pp. 1-26.

Kossow, Niklas, Dykes Victoria (2018): "Blockchain, bitcoin and corruption. A review of the linkages", *Transparency International Anti-Corruption Helpdesk Answer*, 22 january 2018.

Kraft, Timothy J. (2017): "Big Data Analytics, Rising Crime, and Fourth Amendment Protections", *University of Illinois Journal of Law, Technology & Policy*, pp. 249-273.

Laufer, William S. (2017): "The Missing Account of Progressive Corporate Criminal Law", *New York University Journal of Law & Business*, vol. 14, n. 1, pp. 71-142.

Laufer, William S. (2018): "A Very Special Regulatory Milestone", *University of Pennsylvania Journal of Business Law*, vol. 20.2, pp. 392-428.

Levy, Karen E.C. (2013): "Relational Big Data", *Standford Law Review Online*, 73, pp. 73-79.

Lynskey, Orla (2019): "Criminal justice profiling and EU data protection law: precarious protection from predictive policing", *International Journal of Law in Context*, 15, pp. 162-176.

Manacorda, Stefano (2017): "L'idoneità preventiva dei modelli di organizzazione nella responsabilità da reato degli enti: analisi critica e linee evolutive", *Rivista trimestrale di diritto penale dell'economia*, n. 1-2, pp. 49-113.

Mancuso, Enrico Maria (2016): "Le investigazioni interne nel sistema processuale italiano: tra vuoto normativo e prassi applicative incerte", in Centonze Francesco, Mantovani Massimo (eds.): "La responsabilità «penale» degli enti. Dieci proposte di riforma" (Bologna, il Mulino), pp. 217-245.

Manes, Vittorio, Tripodi, Andrea Francesco (2016): "L'idoneità del modello organizzativo", in Centonze Francesco, Mantovani Massimo (eds.): "La responsabilità «penale» degli enti. Dieci proposte di riforma" (Bologna, il Mulino), pp. 137-174.

Mongillo, Vincenzo (2011): "Il giudizio di idoneità del Modello di Organizzazione ex d.lgs. 231/2001: incertezza dei parametri di riferimento e prospettive di soluzione", *La responsabilità amministrativa delle società e degli enti*, III, pp. 69-100.

Mongillo, Vincenzo (2018): "La responsabilità penale tra individuo ed ente collettivo" (Torino, Giappichelli).

Nicolicchia, Fabio (2014): "*Corporate Internal Investigations* e diritti dell'imputato del reato presupposto nell'ambito della responsabilità «penale» degli enti: alcuni rilievi sulla base della «lezione americana»", *Rivista trimestrale di diritto penale dell'economia*, 3-4, pp. 781-809.

Nieto, Adàn Martin (2014): "Internal Investigations, Whistle-Blowing, and Cooperation: The Struggle for Information in the Criminal Process", in Manacorda Stefano, Centonze Francesco, Forti Gabrio (eds.): "Preventing Corporate Corruption. The Anti-Bribery Compliance Model" (Londra, Springer), pp. 69-92.

Olsen, William P. *et al.* (2016): "Using Data Analytics to Meet the Government's Anti-Corruption Compliance Expectations", *The Anti-corruption Report* (www.anti-corruption.com), v. 5, n. 9, may 2016.

Ottolia, Andrea (2017): "*Big Data* e innovazione computazionale" (Torino, Giappichelli).

Paliero, Carlo Enrico, Piergallini, Carlo (2006): "La colpa di organizzazione", *La responsabilità amministrativa delle società e degli enti*, III, pp. 167-184.

Parodi, Cesare, Sellaroli, Valentina (2019): "Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco", *Diritto penale contemporaneo*, 6, pp. 47-71.

Pasquale, Frank A. (2019): "A Rule of Persons, Not Machines: The Limits of Legal Automation", *George Washington Law Review*, 1, pp. 1-60.

Picotti, Lorenzo (2019): "Diritto penale e tecnologie informatiche: una visione d'insieme", in Cadoppi Alberto, Canestrari Stefano, Manna Adelmo, Papa Michele (eds.): "Cybercrime" (Utet, Torino), pp. 35-96.

Piergallini, Carlo (2013): "Paradigmatica dell'autocontrollo penale (dalla funzione alla struttura del "modello organizzativo" ex. d.lg. n. 231/2001)", *Cassazione penale*, 2, pp. 842-867.

Pitaro, Vincent (2018): "Using Data Analytics to Boost Compliance Program Effectiveness", *The Anti-corruption Report* (www.anti-corruption.com), v. 7, n. 13, june 2018.

Pitruzzella, Giovanni (2016): "Big data, competition and privacy: a look from the antitrust perspective", *Concorrenza e mercato*, 1, pp. 15-27.

Ponte, Federico (2017): "I "big data" come "common goods"", *Ciberspazio e diritto*, 1, pp. 31-67.

Proja, Giampiero (2016): "Trattamento dei dati personali, rapporto di lavoro e l'«impatto» della nuova disciplina dei controlli a distanza", *Rivista italiana di diritto del lavoro*, 4, pp. 547-578.

Selvaggi, Nicola (2019): "Compliance, sicurezza informatica e nuove tecnologie", relazione tenuta al Congresso dell'Associazione Internazionale di Diritto Penale – Gruppo Italiano su "*Nuove tecnologie e giustizia penale. Problemi aperti e future sfide*", Teramo, 22-23 marzo 2019.

Severino, Paola (2016a): "Legalità, prevenzione e repressione nella lotta alla corruzione", *Archivio Penale*, 3, pp. 1-8.

Severino, Paola (2016b): "Il sistema di responsabilità degli enti *ex* d.lgs. n. 231/2001: alcuni problemi aperti", in Centonze Francesco, Mantovani Massimo (eds.): "La responsabilità «penale» degli enti. Dieci proposte di riforma" (Bologna, il Mulino), pp. 73-85.

Severino, Paola (2018): "La responsabilità dell'ente ex d.lgs. n. 231 del 2001: profili sanzionatori e logiche premiali", in Paliero Carlo Enrico, Viganò Francesco, Basile Fabio, Gatta Gian Luigi (eds.): "La Pena, ancora, fra attualità e tradizione" (Milano, Giuffrè), pp. 1101-1127.

Severino, Paola (2019): "Strategie di contrasto alla corruzione nel panorama interno e internazionale", *Luiss Open*, 29 marzo 2019.

Starr, Sonja B. (2014): "Evidence-Based Sentencing and the Scientific Rationalization of Discrimination", *Stanford Law Review*, vol. 66, pp. 803-872.

Tebano, Laura (2017): "Employees' Privacy and employers' control between the Italian legal system and European sources", *Labour & Law Issues*, vol. 3, n. 2, pp. 1-20.

Trapani, Matteo (2018): "La prevenzione e il controllo della corruzione e dell'etica pubblica mediante l'utilizzo delle nuove tecnologie", *Forum di Quaderni Costituzionali*, 15 aprile 2018, pp. 1-13.

Tripodi, Andrea Francesco (2013): "L'elusione fraudolenta nel sistema della responsabilità da reato degli enti" (Padova, Cedam).

Vona, Leonard W. (2017): "Fraud Data Analytics Methodology: The Fraud Scenario Approach to Uncovering Fraud in Core Business Systems" (Hoboken, John Wiley & Sons).

Vuona, Bridget (2019): "Foreign Corrupt Practices Act", *American Criminal Law Review*, vol. 53, pp. 979-1032.

Watcher, Sandra, Mittelstadt, Brent (2019): "A right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI", *Columbia Business Law Review*, 2, pp. 1-130.

White, Mary J. (2016): "A New Model for SEC Enforcement: Producing Bold and Unrelenting Results", *Compliance & Enforcement* (wp.nyu.edu), 21 novembre 2016.

Woody, Karen E. (2017): "No Smoke and No Fire: The Rise of Internal Controls Absent Anti-Bribery Violations in FCP Enforcement", *Cardozo Law Review*, vol. 38, pp. 101-139.

Zeno-Zencovich, Vincenzo (2018): "Dati, grandi dati, dati granulari e la nuova epistemologia del giurista", *La rivista di diritto dei media*, 2, pp. 1-7.

Zwiebel, Megan (2017): "Measuring Compliance: Gathering and Analyzing Data", *The Anti-corruption Report* (www.anti-corruption.com), v. 6, n. 18, september 2017.

La partita del diritto penale nell'epoca dei "*drone-crimes*"

El partido del derecho penal en la era de los "delitos de dron"

The Criminal Law Match in the Era Of "Drone-Crimes"

Carla Cucco
Dottoranda di ricerca in cotutela presso l'Università degli Studi di Palermo, corso in "Diritti Umani: Evoluzione, Tutela e Limiti" e presso la Universitat de València (Spagna), corso in "Sostenibilidad y paz en la era posglobal".
carla.cucco@unipa.it

Terrorismo Terrorismo Terrorism

Abstracts

Quale spazio riconoscere alla giurisdizione e al diritto penale italiano nei casi di omicidi mirati a mezzo drone e di *collateral damages* verificatisi nell'ambito della *Global War on Terror,* ad opera degli Stati Uniti d'America in Stati terzi? Alla luce del sempre più frequente impiego dei droni armati come armi altamente tecnologiche e spersonalizzanti nella lotta al terrorismo, si proverà a verificare se e come il diritto penale possa (e debba) muoversi tra le macerie dei *drone strike*: partendo da considerazioni in ordine alla natura del drone e al suo "proficuo" impiego nel contesto sovranazionale, si verificheranno quali sono gli spazi della giurisdizione italiana in materia, specie alla luce del crescente avvalimento di Sigonella come base di decollo dei droni statunitensi e del ruolo della conseguente "segreta" cooperazione italiana nella "lotta al terrore". Successivamente si analizzeranno il segreto di stato e il diniego di ostensione delle *policies* operative, quali vecchi e nuovi ostacoli alla formulazione delle imputazioni e all'accertamento delle responsabilità. Infine, si cercherà di fornire alcune chiavi di lettura dei modi di atteggiarsi del diritto penale, nelle sue dimensioni di antigiuridicità e colpevolezza, rispetto alle possibili (ove individuabili) soggettività coinvolte nella singola operazione di *targeted killing*.

¿Qué margen de maniobra debe darse a la jurisdicción y al derecho penal italianos en los casos de asesinatos selectivos con aviones teledirigidos y de daños colaterales ocurridos en el marco de la Lucha Global contra el Terrorismo, por parte de los Estados Unidos de América en terceros países? A la luz del uso cada vez más frecuente de drones armados como armas altamente tecnológicas y despersonalizadoras en la lucha contra el terrorismo, trataremos de comprobar si y de qué manera el derecho penal puede (y debe) moverse entre los "detritos" de los ataques de estos aviones no pilotados: a partir de consideraciones sobre la naturaleza del dron y su empleo "útil" en el contexto supranacional, se analizarán los ámbitos de la jurisdicción italiana en la materia, especialmente a la luz del creciente uso de Sigonella como base para el despegue de los aviones teledirigidos americanos y el papel de la consiguiente cooperación italiana "secreta" en la "lucha contra el terror". Luego, se analizarán el secreto de Estado y la reticencia a mostrar las políticas operativas de los drones, como viejos y nuevos obstáculos para la formulación de las imputaciones y la determinación de las responsabilidades. Por fin, trataremos de proporcionar algunas claves para la interpretación de las formas de hacer del derecho penal, en sus dimensiones de antijurídicidad y de culpabilidad, con respecto a las posibles (cuando sean identificables) subjetividades involucradas en cada operación de asesinato selectivo.

What space should be given to Italian jurisdiction and criminal law in cases of targeted killings via drones and collateral damages occurring within the framework of the so-called Global War on Terror, waged by the

US in third countries? In the light of the ever more frequent use of armed drones as highly technological and depersonalizing weapons in the fight against terrorism, I will try to verify whether and how criminal law can walk throughout the rubble of drone strikes: after some brief remarks about the drone's nature and its "profitable" employment in the supranational context, the existence of Italian jurisdiction with respect to drone strikes will be discussed, especially in the light of the growing use of Sigonella as a stationing and operating base for US drones and of Italy's "secret" cooperation in the "fight against terror". Subsequently, issues relating to the so-called "secret of State" and the authorities' refusal to disclose operative policies will be tackled, such as both old and new obstacles to the formulation of the imputations and to the individuation of the responsibilities. Finally, will be trying to providing readers with conceptual keys to understand how criminal-law categories – such as justifications and culpability, as well as the proper identification of the authors of the crimes arising from a particular targeted killing – can adapt to such new reality.

Sommario

1. Introduzione.

Se un treno fuori controllo si stesse per dirigere contro cinque uomini legati sulle rotaie, "l'uomo a terra", che ha a disposizione una leva per deviare il treno su un altro binario, la azionerebbe se ciò avesse come effetto quello di uccidere l'unico uomo legato a tale secondo binario? E "l'uomo magro" sul ponte, spingerebbe giù "l'uomo grasso", se il sacrificio di questi fosse l'unica strada possibile per evitare che un altro treno fuori controllo investa i cinque uomini legati sulle rotaie?

Il dilemma giusfilosofico del *trolley problem* (noto anche come *footbridge*) elaborato già nel 1967 da Philippa Foot[1] nelle due versioni innanzi citate e poi approfondito negli anni successivi[2], costituisce il sostrato del controverso dibattito, attuale ed estremamente complesso, sull'ammissibilità dei *collateral damages* di *targeted killings* commessi a mezzo drone, oggi particolarmente rilevanti quali strumenti della *Global War On Terror* di matrice statunitense. In questa complessa materia il ricorso al diritto penale e l'impiego degli istituti classici che lo costituiscono, si intrecciano con valutazioni etiche e questioni internazionalistiche di uso legittimo delle nuove tecnologie nella lotta al terrorismo, di implicazioni lecite o illecite dell'impiego di armi che annientano il pericolo per l'agente, di tutela del diritto alla verità delle vittime: perché, per dirla con Greene, i droni *"fail to push (our) emotional button(s)"*[3], aprendo alla realizzazione di condotte impersonali, distaccate, frutto di scelte puramente cognitivo-utilitaristiche che scardinano il classico approccio personalistico del diritto penale alle fattispecie delittuose.

In metafora, la scelta di azionare la leva, nella prima versione, o di spingere "l'uomo grasso", nella seconda, potrebbe essere intesa come opzione politica dalle cause profonde e profondamente legate al contesto socio-normativo, oltre che dalle ricadute significative in tema di giustificazione delle politiche antiterrorismo nazionali e sovranazionali rispetto ai principi cardine dei sistemi costituzionale e convenzionale dei diritti, e di affermazione delle responsabilità internazionali degli Stati e penali dei singoli. Dilemma che, ad esempio, costituisce l'essenza di una pronuncia del 2005 del Tribunale costituzionale federale tedesco[4], con la quale si dichiarava l'illegittimità della legge federale nazionale sulla sicurezza aerea nella parte in cui legittimava ed autorizzava il Ministro della difesa tedesco ad ordinare all'aeronautica militare l'abbattimento di un aereo civile, in caso di necessità, ove vi fosse stato il sospetto del suo impiego "contro la vita di esseri umani" (art. 14, co. 3, del *Luftsicherheitsgesetz* dell'11 gennaio 2005). Il *Bundesverfassungsgericht* si intromette nella scelta adottata dal legislatore tedesco nella direzione (positiva) di "azionare la leva" e di "buttare l'uomo grasso", opponendo a questa i limiti invalicabili del diritto alla vita e dell'intangibilità della dignità dell'uomo. La generica autorizzazione ad abbattere aerei civili, trasportanti equipaggio e passeggeri innocenti, nel caso in cui essi siano dirottati da presunti terroristi per colpire obiettivi civili o militari, farebbe oscillare il pendolo del dilemma a danno dei "pochi", soppesati come "costo sopportabile" per evitare la morte dei "molti", svuotando i primi della loro natura di uomini liberi e rendendoli oggetti nelle mani dei più "forti" (indifferentemente terroristi e/o Stati).

L'opzione del legislatore tedesco nel senso dell'ammissibilità dell'evento morte delle vittime collaterali, ove la gravità della minaccia rappresentata dal velivolo compensi, in termini di proporzionalità, la scelta di azione militare, costituisce una giustificazione normativa *ex ante* delle scelte amministrative compiute *case by case* per scopi di lotta al terrorismo e di protezione della sicurezza interna.

[1] Foot (1967), pp. 5-15, disponibile al seguente *link*: *Philpapers.org*.
[2] Thomson (1985), pp. 1395-1415, disponibile su *Jstor.org*; Greene (2007), pp. 35-80, a questa *pagina*.
[3] Greene (2007), pp. 43 e 76.
[4] BVerfG - 1 BvR 357/05, per cui si veda Siciliano (2008), pp. 173-176.

Ma la prospettiva assunta dalla Corte risulta altresì rilevante in questa sede per le argomentazioni addotte: la stessa, lungi dal contestare la scelta legislativa sul piano della *ratio* di lotta al terrorismo e dal compiere valutazioni circa la pericolosità del suddetto fenomeno sul piano interno ed internazionale, si concentra sull'incompatibilità costituzionale della soluzione legislativa proposta con il principio della dignità dell'uomo e con il diritto alla vita genericamente garantito. La posizione della Corte, che si muove nel senso della preminenza della tutela dei diritti delle vittime dell'attacco sulle esigenze di sicurezza nazionale, pare giustificata dalla circostanza che la scelta normativa adottata non risultasse "emergenziale" in quanto compendiata in un atto normativo destinato a stabilizzarsi ed a "normalizzarsi"[5]. Un problema di bilanciamento di non agevole soluzione e che attraversa, del vero, l'intera legislazione antiterrorismo di molti Stati liberali.

Come detto, la Corte nelle sue argomentazioni non presta sufficiente attenzione alla finalità della normativa dichiarata illegittima; la quale, invece, risulta di centrale rilevanza, poiché in essa emerge la *voluntas* legislativa di evitare che il diritto penale possa essere chiamato in causa per conoscere della responsabilità di chi, all'apice o alla base della gerarchia militare, dia l'ordine di attacco o lo sferri. Intervenire a monte è funzionale ad eludere le difficoltà estreme di un accertamento penale che, difficile in ordine alle valutazioni delle autorità militari nazionali, risulta quasi impossibile ove si discuta di scelte compiute da organi militari o, vieppiù, da servizi di *intelligence* stranieri.

E tanto appare ancora più complesso ove si discuta di omicidi mirati a mezzo drone e dei relativi *collateral damages*, alla luce della natura altamente tecnologica di tali nuove armi, della spersonalizzazione di cui si fanno portatrici e delle peculiarità insite nel loro impiego, con ricadute di ovvia rilevanza nella prospettiva dell'apertura di un processo penale che veda al banco degli imputati oggetti semi-autonomi, i cui "gestori" restino nell'ombra. Ed ecco che qui "l'uomo a terra" e "l'uomo magro" diventano protagonisti assoluti e paradossalmente dotati di libero arbitrio: la scelta di tirare la leva o di spingere "l'uomo grasso" si fa consapevole, ponderata, addirittura frutto di una strategia antiterrorismo specifica, in cui si anticipa l'arrivo di un possibile treno fuori controllo. Il *trolley problem* si tende fino all'estremo, quasi alla rottura, e di esso si pone in luce un aspetto innovativo, legato all'ammissibilità della consapevole scelta di "uccidere uno per salvarne cinque" che si fonda sull'ipotetico, futuro, possibile "treno del terrorismo" non ancora minaccioso in concreto.

2. *AI* e droni: spersonalizzazione e crisi delle categorie giuridiche classiche.

Il paradigma penalistico classico del reo come agente-persona fisica pare oggi in crisi: il progresso tecnologico agevola la commissione dei crimini e rinsalda le aspirazioni di non punibilità dei loro autori, rendendo più difficile la concreta dimostrazione della loro riconducibilità a persone fisiche determinate. La veridicità dell'assunto si coglie in modo lampante con riguardo all'impiego di intelligenze artificiali, in cui l'apporto umano è compresso al punto, in alcuni casi, da scomparire. Ed è parimenti comprensibile anche rispetto all'uso dei droni, che pur afferendo alla categoria suddetta, rispetto alle *Artificial Intelligence (AI)* "pure", non annullano *in toto* la cooperazione umana alla loro attivazione, al controllo e alla gestione: in questi casi la spersonalizzazione passa invece attraverso la mancata ostensione di documenti, dati relativi alle operazioni a mezzo drone, attribuzione di incarichi. Si intende sostenere, cioè, che sebbene la separazione tra uomo a macchina nel drone non sia netta, la stessa diventa tale in via "burocratica", nella misura in cui in spregio al principio di trasparenza e a quello di collaborazione tra gli organi giurisdizionali si occultano le informazioni utili sia ai cittadini, per conoscere i diretti responsabili di condotte lesive di propri interessi o diritti, sia agli organismi investigativi e alle Corti, per lo svolgimento di attività di indagine e l'incardinazione di

[5] In questi termini Bin (2007), pp. 39-54, secondo cui: *"L'ordinamento ha spesso cercato di inglobare nella "regola" l'eccezione: la teoria della necessità come fonte suprema dell'ordinamento, l'"invenzione" della decretazione d'urgenza, la stessa disciplina dello stato d'assedio ne sono la riprova"* (p. 41); e ancora *"l'emergenza causata dal pericolo esterno giustifica misure restrittive dei diritti che poi vengono applicate nella gestione "ordinaria" di vicende interne"* (p. 44); De Vergottini (2004), pp. 1185-1211. Si può qui osservare che la Corte Costituzionale italiana in una sua risalente pronuncia (C. cost., sent. n. 15/1982) aveva affermato la competenza statale *("non solo il diritto e il potere ma anche il preciso e indeclinabile dovere")* all'adozione di una normazione dell'emergenza, chiarendo però che l'ingiustificata protrazione nel tempo delle stesse misure ne avrebbe fatta venir meno la legittimità.

processi penali[6].

Le *AI* sono delle macchine dotate di intelligenza autonoma, che riproducono le caratteristiche umane e che prescindono dalla coscienza ai fini del loro funzionamento, operando in sostanza come *decision makers*[7]; la totale spersonalizzazione della macchina pone problemi, a monte, di attualità delle categorie penalistiche e, a valle, di ascrizione delle responsabilità, in particolare sotto il profilo dell'imputabilità e del riconoscimento degli elementi soggettivi di dolo e colpa e dei profili a questi ultimi inerenti della volizione e prevedibilità degli effetti lesivi. Del resto il problema della responsabilità, già complesso nel caso in cui il reato sia riconducibile ad intelligenze artificiali impiegate nella quotidianità delle moderne società tecnologiche, presenta ulteriori profili di criticità quando gli illeciti vengano commessi in contesti di guerra e della macchina-soldato si faccia un uso in via sostitutiva o alternativa ai militari "in carne ed ossa"[8], poiché capaci di incidere positivamente sul decorso della guerra in due modi: limitando l'esposizione fisica dei soldati al pericolo, e determinando in essi una maggiore inclinazione ad uccidere innocenti (o comunque meri sospetti nemici o terroristi) senza essere esposti ad alcun rischio di incriminazione.

La stessa Unione Europea ha acquisito piena consapevolezza degli effetti dannosi dell'uso indiscriminato di intelligenze artificiali autonome: in tal senso il Parlamento Europeo con una risoluzione del 2017[9], nonostante affronti il tema sul versante della responsabilità civile, effettua delle considerazioni di più ampio respiro, capaci di incidere anche in una prospettiva penalmente rilevante. Evidenzia infatti l'esistenza di una relazione di proporzionalità decrescente tra l'uso di intelligenze sempre più "inumane" e la sufficienza delle tradizionali regole in materia di responsabilità per condotte imputabili ai *robot*. Tanto sulla scorta della carenza di uno *status* giuridico che li comprenda (non sono persone, né enti, né altri soggetti di diritto): di talché centrale appare per il Parlamento la necessità di delineare a livello eurounitario una nuova categoria di genere *"con caratteristiche specifiche e implicazioni proprie"* (cfr. considerando AC), *"[…]di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei robot che prendono decisioni autonome o che interagiscono in modo indipendente con terzi"* (Art. 59 lett. f).

Parzialmente diversa, ma non meno discussa, è la questione della responsabilità per fatto derivante da utilizzo di droni, in particolare ove gli stessi vengano impiegati come armi idonee a cagionare eventi lesivi penalmente rilevanti[10]: rispetto alle altre forme di *AI*, ancorché i droni siano suscettibili di annullare la vicinanza (fisica e psichica) tra autore dell'attacco e la vittima, non assumono pienamente la fisionomia di *decision makers*. La differenza non ha ricadute esclusivamente sostanzialistiche, in termini descrittivi e delineativi del sistema penale moderno e dell'attualità delle sue categorie (tra tutte, nel caso di specie, quelle dell'imputabilità e della colpevolezza), ma altresì sotto il profilo processuale del riconoscimento e dell'imputazione soggettiva di eventuali responsabilità (civili e penali).

Con riguardo al particolare settore dell'impiego dei droni armati come armi della *Global War on Terror*, in via teorica e ad un primo sguardo parrebbe agevole sostenere che la responsa-

[6] Si potrebbe cioè ritenere che la *disclosure* non sia utile solo per scopi investigativi, ma anche per garantire un dialogo sociale produttivo sul tema, che possa influenzare l'impiego di tali strumenti e la scelta di assistenza a Stati che ne facciano uso: ad esempio, il Rapporto di ricerca Iriad (2017) (chiarisce che *"Le inchieste demoscopiche mostrano posizioni ampiamente critiche nei confronti della strategia americana. Le rilevazioni del Pew Research Center, infatti, mettono in luce una diffusa contrarietà all'impiego dei droni armati statunitensi per colpire presunti terroristi in aree di crisi. Si evidenzia, nel complesso, che ben 17 Paesi sui 20 analizzati nel 2012 e addirittura 39 sui 44 analizzati nel 2014 sono nettamente contrari"* (p. 109): si tratta invero di un dato relativo alla comunità internazionale che non tiene conto del diffuso sostegno che invece la campagna di *drone strike* statunitense trae dal consenso dei cittadini americani.

[7] Hallevy (2010), pp. 171-201. Si fa qui riferimento agli arti bionici e ai *cyborg*, il cui sviluppo risolve in svariati campi del sapere numerosi problemi (basti pensare proprio all'uso degli arti bionici per garantire il recupero completo e un normale stile di vita a chi abbia perduto quelli naturali, o l'impiego di macchine autonome e non controllate per la produzione, idonee a snellire le tempistiche dei processi e a ridurre i rischi alla sicurezza di persone e cose, o ancora l'impiego ormai diffuso di *robot* da cucina), benché altrettanti ne pone sul terreno del diritto penale. Tema in ogni caso eccentrico rispetto a quello qui affrontato delle armi autonome e che come tale non potrà essere approfondito.

[8] Si pensi all'uso militare dei cd. *robot killer SGR-A1*, impiegati per scopo difensivo dei confini dalla Corea del Sud e rispetto ai quali è discussa la completa autonomia decisionale (secondo il modello dello *HOLT-Human on the loop*) che, se confermata, contrasterebbe con le posizioni contrarie all'*HOTL* assunte in sede internazionale da organismi istituzionali (nella specie, quelle del *Committee on International Security and Arms Control* e della Corte Penale Internazionale) e *watch dogs* a tutela dei diritti umani (come lo *Human Rights Watch*): cfr. Pike (2011); Velez-Green (2015); Weinberger (2014).

[9] *Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica* (2015/2103(INL)), disponibile all'indirizzo dell'*Europarlamento*. Per una analisi della Risoluzione si veda Berto (2017).

[10] Meloni (2017), pp. 145-148.

bilità sia senz'altro da addebitare astrattamente al soggetto responsabile dell'attacco che abbia prodotto effetti lesivi "fuori *target*". Ma la teoria non coincide con la realtà, molto più complessa e fumosa, dalla quale sorgono tre ulteriori quesiti connessi: (i) chi è, nella catena di comando della singola operazione di attacco antiterrorismo tramite drone, il soggetto cui la responsabilità va ascritta?; (ii) Che differenza sussiste, ai fini del corretto incardinarsi del processo penale e della chiara formulazione dell'imputazione, tra (ii.1) il caso in cui la responsabilità attenga a casi di *drone strike* in cui la morte delle vittime collaterali sia frutto di un "errore" della macchina (salvo non lo si ritenga un errore di programmazione comunque riconducibile all'uomo, e anche in tale caso il problema resta identico: chi è questo "uomo"?) e (ii.2) il caso in cui le vittime non designate siano attinte sì in via collaterale ma quali conseguenze di un attacco "ben" sferrato sul *target*?; (iii) È possibile riconoscere sussistente una responsabilità (e in capo a quali soggetti) anche rispetto agli illeciti commessi ai danni degli stessi *target* terroristici?

Sebbene non si pretenda in questa sede di dare risposte univoche e assolute ai citati quesiti e agli altri che via via emergeranno nel prosieguo (peraltro, nella piena consapevolezza delle notevoli sfaccettature del tema che richiederebbe lo sforzo congiunto dei giuristi di ogni settore del diritto), si tenterà di fornire degli spunti di riflessione sulle ricadute nel settore penale dell'uso dei droni armati in chiave di *counterterrorism*, specie prevedendosi (senza tuttavia auspicarlo) un loro uso sempre più frequente ed indiscriminato.

3. Le implicazioni dei *drone strike* nella *Global War on Terror*.

La particolare natura del drone armato ed il suo caratteristico funzionamento giustificano il larghissimo uso che di esso si è fatto sia in ambito civile sia, in particolare per ciò che attiene all'analisi che in questa sede si intende compiere, in ambito militare e come strumento di *counterterrorism* ad opera prevalentemente degli Stati Uniti d'America[11].

Quale la peculiarità del sistema, croce e delizia a seconda della prospettiva dalla quale si guarda, che ne ha giustificato un impiego sì massiccio?

I droni, nella denominazione italiana "aeromobili a pilotaggio remoto" (APR) -nella dicitura anglosassone *Remotely Piloted Aircraft System* (*RPAS*), distinti quanto a funzioni e peso dalle classi degli *Unmanned Aircraft System* (*UAS*) - sono velivoli privi di pilota umano e quindi "*automated*", cioè guidati a distanza[12]. La loro automazione, in ogni caso, non vale autonomia: di tali droni permane infatti il controllo umano a monte, sicché il riferimento al pilotaggio remoto è funzionale a mettere in luce il coinvolgimento umano in tutte le decisioni critiche che vengono assunte nel corso delle varie missioni[13]. Quelli utilizzati per scopi letali sono di tipo *Predator* e *Reaper*[14] e sono impiegati nella lotta al terrorismo come droni *hunter-killer*, deputati all'assolvimento di plurime funzioni: di *intelligence*, sorveglianza, ricognizione delle aree sensibili, individuazione del bersaglio e *strike*[15]. Il drone, infatti, pensato in prima istanza come strumento discreto e certamente grandemente efficace per il compimento di attività di videoregistrazione delle aree "sensibili", frequentate da presunti terroristi, può essere però operato, sempre da remoto, per colpire *target* selezionati con sufficiente precisione, installando sul velivolo missili di precisione, tendenzialmente di tipo *Hellfire*.

La distanza che pertanto si frappone tra l'operatore, il personale di controllo e l'area di azione del drone, in aggiunta all'efficace attitudine a colpire ed eliminare sospetti terroristi (individui o interi gruppi), riduce i rischi per gli agenti impegnati nella sua gestione, allenta i

[11] In verità, i droni come armi hanno ricevuto analogo impiego anche ad opera di Regno Unito e Israele. Sulla legalità dei *targeted killings* si veda la pronuncia *Public Committee against Torture in Israel v. Israel*, case No. HCJ 769/02 (The Supreme Court, Israel, December 14, 2006).

[12] In modo essenziale, è possibile trarre definizioni e chiarimenti sulle modalità di impiego e funzionamento dei droni armati dal manuale militare *Unmanned Aircraft Systems* (2017), disponibile al seguente *link* (il quale sostituisce il manuale precedente *The UK Approach to Unmanned Aircraft Systems* (2011), oggetto di critiche, rinvenibile a questo *indirizzo*). In particolare per la divisione in classi di droni in relazione alle funzioni svolte, si attenzioni la tabella 2.5 di cui a pag. 18 del manuale *Unmanned Aircraft System*.

[13] I droni dei quali si discute in questa sede, impiegati cioè nelle attività di *targeted killings*, sono come detto automatici ma non autonomi: distinzione che risulta ben espressa alla tabella 2.3, pag. 13 del manuale *Umanned Aircraft System*, citato alla nota precedente. Non si affronterà in questa sede la diversa classe dei droni totalmente autonomi, i cui problemi in relazione all'accertamento di eventuali responsabilità per fatti illeciti sono evidentemente affini a quelli che si pongono per le *AI* e dei quali, per evidenti ragioni di pertinenza, non si potrà dar conto in questa sede.

[14] Dati precisi sulle tipologie di droni sono disponibili alla pagina *web* dell'*Understanding Empire: Technology, Power, Politics*: *Understandingempire.wordpress*.

[15] Si veda il Rapporto Iriad (2017), citato alla nota n. 6.

freni inibitori legati al suo utilizzo ed impedisce l'attivazione dei normali meccanismi tipici di un attacco armato (quale, ad esempio, la comunicazione con la persona bersaglio), così motivando il larghissimo impiego di droni nella *Global War on Terror*[16].

Proprio la logica della *Global War on Terror*, complessa e a tratti intelligente (per le finalità che gli Stati Uniti intendono perseguire e gli effetti giuridici che mirano a (non) realizzare, come si cercherà di chiarire nel prosieguo), costituisce lo sfondo e il cuore della problematica sulla possibile qualificazione dei *targeted killings* ad essa riconducibili come crimini contro l'umanità o crimini di guerra, e quindi il riconoscimento di responsabilità statali-internazionali e individuali-penali: l'assunto irrisolto di fondo è infatti quello della controversa riconducibilità del *drone strike* al regime del diritto di guerra o *international humanitarian law* (d'ora in poi *IHL*), o a quello di pace in chiave di *law enforcement*, che fa capo al sistema penale interno.

Intesa come azione bellica antiterrorismo, formula in cui, con deliberata maliziosa scorrettezza, si associano i concetti distinti di guerra e antiterrorismo[17], la *Global War on Terror* è assunta come giustificazione dei *drone strikes*, allo scopo di evitare che le attività ad essa ascrivibili siano assoggettate alla normativa del diritto internazionale dei diritti umani, a tutto vantaggio dell'applicazione delle norme maggiormente permissive dell'*IHL* (con il suo portato dell'operatività dei principi di proporzionalità e necessità dell'attacco che consentirebbero di giustificare le uccisioni collaterali come "ragionevoli incidenti di guerra", la possibilità di sfruttare le immunità valide per i militari o le maggiori aperture che l'*IHL* garantisce ad un uso della forza extraterritoriale tanto elastico da ammettersi addirittura come strumento di autodifesa preventivo)[18].

La difficoltà di leggere le operazioni antiterrorismo attraverso la lente della guerra in senso tradizionale emerge con evidenza in relazione ai *drone strikes* statunitensi, ove l'azione lesiva si manifesta fuori dal territorio americano, benché ivi siano localizzate le decisioni assunte e si teme possano prodursi le conseguenze paventate e avversate.

Non si può dare in questa sede conto delle ragioni che inducono a ritenere ascrivibili nell'ambito delle operazioni di *law enforcement* gli attacchi statunitensi a mezzo drone commessi in Yemen, Somalia e Pakistan (escludendo quindi quelli di Iraq e Afghanistan, di numero certamente più limitato e verificatisi nell'ambito di conflitti armati)[19]: rinviandosi alla puntuale letteratura internazionalistica esistente sul punto[20], si osserva qui come la condivisione degli assunti da essa prospettati, apre alla possibile operatività degli istituti di diritto penale per l'accertamento delle responsabilità individuali e delle regole di diritto internazionale dei diritti umani per la possibile qualificazione dei *targeted killings* e, *a fortiori*, dei *collateral damages*, come crimini di guerra e crimini contro l'umanità.

Ritenendo quindi che sia giuridicamente scorretta la qualificazione della *Global War on Terror* come conflitto armato (ed è per tale ragione che, ad esempio, non si parlerà mai in questa sede di azione bellica antiterrorismo, né si ricorrerà al concetto di "civile" parlando dei *target* non selezionati), ma che si tratti di uso extraterritoriale della forza, si pone il problema di stabilire in che termini questo si giustifichi, da quale autorità provengano gli ordini di azione,

[16] La citata formula fu utilizzata per la prima volta nel corso del Congresso del 12 settembre del 2001 dall'allora Presidente degli Stati Uniti George W. Bush (la trascrizione dell'intervento è accessibile a questo *indirizzo*); si colloca in data 14 settembre del 2001 l'adozione ad opera del Congresso della *Authorization for the Use of Military Force* (AUMF) (a questo *link*), firmata 4 giorni dopo dal Presidente degli Stati Uniti, con la quale si (auto)legittima l'esercizio della forza extraterritoriale per esigenze di tutela della sicurezza americana dal pericolo terroristico.

[17] Per una critica maggiormente analitica all'assimilazione tra guerra e terrorismo si rinvia a Cucco e Mauri (2018), pp. 65-90.

[18] Già nel 2006 la Corte Suprema degli Stati Uniti ha escluso la giurisdizione del tribunale militare soggetti sospettati di avere legami con Al-Qaeda detenuti a Guantanamo (cfr. 548 U.S. 557 (2006) – Hamdan v. Rumsfeld, Secretary of defence et al. – disponibile *qui*): la decisione della Corte implica la qualificazione degli stessi come civili o prigionieri di guerra e non come combattenti illegali, aprendo le porte alla giurisdizione ordinaria. Diversamente la già citata pronuncia del 2002 della Suprema Corte Israeliana (*Public Committee against Torture in Israel v. Israel*, case No. HCJ 769/02 (The Supreme Court, Israel, December 14, 2006)) la quale, a fronte della tesi sostenuta dal governo israeliano, circa la qualificazione dei membri di organizzazioni terroristiche attivi in Israele in termini di "combattenti illegali in un conflitto bellico", in quanto tali, obiettivi legittimi, pur qualificando le lotte intestine tra governo e terroristi come conflitto armato, ha escluso che i terroristi potessero intendersi come combattenti e tantomeno come civili, usando la più criptica formula di "combattenti non legali". La Corte esclude pertanto la possibilità di ammettere in termini assoluti la legalità delle uccisioni mirate commesse ai danni di presunti terroristi (par. 60), assoggettandone l'ammissibilità al ricorrere di quattro condizioni da accertare *case by case* (par. 40): (i) la decisione di uccidere deve essere basata su prove attendibili; (ii) la misura dell'uccisione mirata deve essere proporzionata; (iii) l'attacco deve essere seguito da un'indagine approfondita; (iv) il danno collaterale deve essere proporzionato.

[19] Melzel (2008), p. 42. In verità la stessa *Presidential Policy Guidance* (*PPG*) di Obama, della quale si parlerà, individua il suo campo di applicazione "*outside of areas of active hostilities*", escludendo quindi implicitamente l'esistenza di un conflitto bellico tra Stati Uniti e Al-Qaeda.

[20] Tramontana (2018), n. 1, pp. 53-75; Lubell e Dereiko (2013), pp. 65–88; Lubell (2012), pp. 421-454.

a che livello di insindacabilità si collochino le direttive impartite per ogni singolo attacco e che considerazione rivestano i *target* selezionati e le vittime collaterali in ambito internazionale.

La Casa Bianca, per il tramite della *CIA*, ha avviato una campagna ormai stabile di *targeted killings* sotto l'egida della cd. dottrina Obama-Clinton[21], usata come pretesto per ritenere applicabili (benché sia controverso che ciò sia possibile), le regole più elastiche dell'*IHL*, in assenza di un'autorizzazione dallo Stato territoriale ove gli attacchi vengono sferrati e nell'impossibilità di affermare l'esigenza della legittima difesa *ex* art. 51 della Carta delle Nazioni Unite[22].

Il dubbio che pare affiorare, già nelle prime battute di questa analisi, è che l'ambito di applicazione del diritto penale sia più esteso di quanto a primo impatto possa apparire: che possa quindi ammettersi l'imputabilità di responsabilità penali in capo ai soggetti della catena di comando coinvolti nei *drone strikes* non solo per gli omicidi collaterali ma anche per quelli dei sospetti terroristi, vittime designate?

A differenza della guerra nella sua tradizionale accezione e portata, l'attività di *counter-terrorism* compiuta mediante l'uso di droni armati non è condotta attraverso attacchi spersonalizzati sul territorio nemico, ma come assalto mirato al terrore: ogni attacco è infatti individualizzato, personalizzato in relazione allo specifico sospettato terrorista e alle contingenze spaziali e temporali in cui si scelga di mandare a segno lo *strike*. La decisione circa il soggetto destinatario delle attività di monitoraggio, prima, e delle uccisioni mirate, poi, avviene tendenzialmente ricorrendo alle *black list* redatte dal Dipartimento di Stato americano, poi compendiate in apposite liste approvate dal Presidente degli Stati Uniti[23]. Aver introdotto in tale paese la categoria degli *enemy combact*s con riferimento ai terroristi ha avuto il vantaggio di sottrarre i sospetti terroristi sia alle regole del diritto penale, sia a quelle dell'*IHL* proprie dei prigionieri di guerra, ampliando la sfera di discrezionalità dell'esecutivo[24], attraverso quanto previsto da apposite *policies*, in specie la *Presidencial Policy Guidance (PPG)* della presidenza Obama e le regole contenute nella *Principles, Standards, and Procedures* (*PSP*) ancora non ufficialmente ostesa, del Presidente degli Stati Uniti Donald Trump (entrambe oggetto di analisi specifica al § 5 in tema di responsabilità individuali per *drone strike*).

Tale scenario normativo non risulterebbe del tutto compatibile con l'approccio assunto dalla disciplina italiana in materia di terrorismo, poiché l'impiego degli strumenti del diritto penale, ancorché in una chiave di punibilità anticipata, dimostra che la logica bellica del terrorista come nemico è rigettata, e il processo penale si atteggia come strumento di difesa sociale[25].

[21] Si tratta della dottrina secondo la quale l'azione statunitense consistente nell'impiego della forza extraterritoriale in tanto si legittima in quanto la minaccia terroristica continui ad essere presente e viva e costituisca pericolo significativo per gli Stati Uniti e la sua popolazione (cfr. Koh (2010)). Sul tema dell'individuazione del regime giuridico applicabile ai *targeted killings* statunitensi si veda Meloni (2017); Cucco e Mauri (2018), p. 67 e ss..

[22] Legittima difesa che invece si addusse e riconobbe nel caso dell'intervento statunitense in Afghanistan dopo i fatti dell'11 settembre 2001 (si veda Consiglio di Sicurezza, risoluzione n. 1368 (2001), S/RES/1368 (2001), sul sito dell'*Onu*, secondo cui *"Insta a todos los Estados a que colaboren con urgencia para someter a la acción de la justicia a los autores, organizadores y patrocinadores de estos ataques terroristas y subraya que los responsables de prestar asistencia, apoyo o abrigo a los autores, organizadores y patrocinadores de estos actos tendrán que rendir cuenta de sus actos; 4. Exhorta a la comunidad internacional a que redoble sus esfuerzos por prevenir y reprimir los actos de terrorismo, entre otras cosas cooperando más y cumpliendo plenamente los convenios internacionales contra el terrorismo que sean pertinentes y las resoluciones del Consejo de Seguridad, en particular la resolución 1269 (1999), de 19 de octubre de 1999"*). Per maggiori approfondimenti si rinvia a Cucco e Mauri (2018), p. 68, nota n. 9.

[23] Le liste delle Organizzazioni Terroristiche Straniere (*Foreign Terrorist Organizazions – FTOs*) designate dal Segretario di Stato dagli Stati Uniti d'America sono accessibili sul sito *governativo americano*.

[24] Viganò (2006), pp. 658-659.

[25] Un problema ulteriore che il tema potrebbe porre, ma che per esigenze di coerenza del testo si ometterà di indagare compiutamente, è quello della rilevanza ai fini del diritto penale interno della qualificazione in termini di "sospetto terrorista" di chi sia oggetto del *listing* citato ad opera di uno Stato straniero o dello stesso Stato del giudizio, con la conseguenza che, ove affermata, escluderebbe l'applicazione delle norme di diritto penale ai casi di *drone strikes* commessi proprio *on target*. Sulla rilevanza delle *black lists* nel sistema nazionale si rinvia in dottrina a Viganò (2007), p. 392; Oliveri Del Castillo (2005), p. 79; Della Morte (2009), p. 443-475; Di Stasio (2010), p. 599-602; in giurisprudenza: Cass. pen., Sez. I, sent. n. 35427 del 21 giugno 2006, Drissi, in *Cass. pen*., 2007, p. 1578 ss. con nota di Cerqua (2007); Cass. pen., Sez. 1, sent. n. 30824 del 15 giugno 2006, imp. Tartag; Cass. pen., Sez. I, sent. n. 1072 del 11 ottobre 2006, imp. Bouyahia ed altri, altresì richiamata da Trib. Roma, Gip, ord. 18/07/2015, RG 15661/2012. In quella sovranazionale: *Sison c. Consiglio*, 26 aprile 2005 (cause riunite T-110/03, T-150/03 e T-405/03); *Kadi c. Consiglio e Commissione*, 21 settembre 2005 (T-315/01); *Yusuf e Al Barakaat International Foundation c. Consiglio e Commissione*, 21 settembre 2005 (T-306/01).

4. Possibili spazi di manovra della giurisdizione penale italiana.

Occorre in primo luogo comprendere in che termini possa sostenersi e radicarsi la giurisdizione penale italiana rispetto ai casi di *targeted killings*. Affermazione della giurisdizione che, in ultima istanza, vale come riconoscimento dei diritti delle vittime, ed in specie del diritto a chiedere ed ottenere una tutela innanzi ad un organo imparziale e indipendente, e che risulta altresì funzionale ad evitare che siano ad essa sottratti i responsabili di fatti penalmente rilevanti.

Tre sono i livelli spaziali da tenere in considerazione ai fini della presente analisi: (i) qual è il luogo da cui il drone decolla?; (ii) quale quello in cui il drone sferra l'attacco?; (iii) in che territorio si trova la cabina di regia, dalla quale il drone è materialmente pilotato?

Gli stessi si combinano con ulteriori tre livelli soggettivi: (a) qual è lo Stato "della bandiera"?; (b) quale lo Stato della "pista di lancio" del drone?; e (c) quale la nazionalità delle vittime (collaterali e selezionate)?

Dal combinarsi di tali piani emergono tre possibili tipologie di giurisdizione penale per *drone strikes*: omicidio mirato in territorio italiano, commesso contro cittadini italiani o stranieri; fatto commesso in territorio straniero contro un cittadino italiano, sia ad opera di droni italiani o di Stati terzi; fatto commesso in territorio straniero con drone decollato dal territorio italiano.

Omettendo l'analisi della prima ipotesi, che pare di minor pregio in quanto ancora – e si spera ancora a lungo - solo di ipotetica verificazione, la seconda ipotesi ha trovato applicazione con riguardo al caso Lo Porto, sul quale, a seguito di una prima richiesta di archiviazione del 29 maggio 2017, rigettata del Gip del Tribunale di Roma[26], è seguita una seconda analoga richiesta (n. 3534/12 R.I. P.M.) sulla quale, alla data in cui scrive, pende la riserva sulla decisione del Gip. Basti qui osservare che il legislatore ha voluto tentare la strada della competenza "specializzata" deferendo, ai sensi del comma 1 *bis* dell'art. 10 c.p.p., la competenza al Tribunale o alla Corte di Assise di Roma, in tutte quelle situazioni, tra cui parrebbe rientrare anche la presente, nelle quali risulti impossibile definire la competenza *ex* comma 1 dello stesso articolo e tanto sempre che non ricorrano casi di connessione o procedimenti collegati.

La terza ipotesi è però quella certamente più interessante: si configura in particolare in tutti i casi di impiego dell'aeroporto militare di Sigonella, in Sicilia, come base operativa di droni italiani e statunitensi[27].

Ai sensi del comma 2 dell'art. 6 c.p. si intende commesso in territorio italiano il reato la cui azione o omissione costitutiva sia avvenuta in tutto o in parte in esso, o ivi si sia prodotto l'evento[28]. Ora, ammettendo che il reato si perfezioni certamente in territorio straniero, e ferme restando le condizioni di cui all'art. 10 c.p., resta da comprendere quando possa dirsi iniziata l'esecuzione dello stesso: in termini più chiari, rimane da stabilire se l'azione del lancio del missile dal drone si esaurisca in se stessa o se afferisca all'azione come componente necessaria tutta la fase di volo del drone a partire dal decollo.

In questa sede sarà solo possibile costruire ipotesi, specie considerando la spessa e ampia coltre di nebbia che copre la materia. Ad oggi è noto esclusivamente il fatto che l'Italia abbia concluso con il Governo degli Stati Uniti un accordo di avvalimento da parte di quest'ultimo della base di Sigonella[29]; tale documento si affianca a precedenti accordi, tra i quali il *"Technical Arrangement on Sigonella"*[30] con il quale si fissano sul piano tecnico le regole di ripartizione delle competenze tra Italia e Stati Uniti.

Ai presenti fini è centrale la precisazione contenuta in quest'ultimo documento secondo la quale *"(t)he U S. Commander has full military command over U S personnel, equipment and operations He will notify in advance the Italian Commander of all significant U S activities, with specific*

[26] Il provvedimento in discorso è il 159948/17 R.Gip, del 02.03.2018, reso nel procedimento n. 3534/12 RG.NR, a scioglimento della riserva formulata in esito all'udienza del 30 gennaio 2018 sull'opposizione alla richiesta di archiviazione avanzata dalla Procura di Roma.
[27] Per un'analisi internazionalistica *ante litteram* si rinvia a Mauri (2016), pp. 319-325.
[28] Si veda da ultimo Cass. pen, Sez. 6, sent. n. 20513 del 19 gennaio 2018, p. 4; Cass. pen., Sez. 3, sent. n. 35165 del 18 luglio 2017, Sorace; Cass. pen., Sez. 4, sent. n. 6376 del 20 gennaio 2017, Cabrerizo Morillas, Rv. 269062; Cass. pen., Sez. 5, sent. n. 570 del 08 novembre 2016, Figliomeni, Rv. 268599; Cass. pen., Sez. 2, sent. n. 48017 del 13 ottobre 2016, Di Luca, Rv. 268432; Cass. pen., Sez. 6, sent. n. 13085 del 03ottobre 2013, Amato, Rv. 259486 (tutte le pronunce citate nel presente scritto, in assenza di diversi riferimenti, sono state consultate sul sito *Italgiure*).
[29] Di tale "quieto" accordo da notizia il *Wall Street Journal* in un articolo dall'eloquente titolo *Italy Quietly Agrees to Armed U.S. Drone Missions Over Libya* (Lubold e Barnes (2016)).
[30] Documento disponibile al seguente *link*.

reference to the operational and training activity" (Sez. IV, art. 3): in altri termini, nonostante la competenza delle operazioni militari sia statunitense, resta fermo un obbligo di notifica all'autorità italiana di tutte le attività statunitensi *"significant"* ad esclusione delle attività di *routine* (come chiarito nell'*Annex* n. 5, capo 1, lett. b), n. 1), ove si legge che *"(t)he term significant is intended to exclude all routine activities"*. Ad esso si oppone il potere del *Commander* italiano di *"(i)ntervene to have the U.S Commander immediately interrupt U.S. activities which clearly endanger life or public health and which do not respect Italian law"* (capo 1, lett. c), n. 7).

Ora, muovendo dalla natura tuttora segreta dell'accordo, dal fatto che le uniche informazioni ostese sono quelle del *Technical Arrangement* e dal dato secondo cui l'unica notizia ulteriore, per bocca dell'allora ministra Pinotti, è che l'uso dei droni nei *targeted killings* sia *"di volta in volta discusso ed autorizzato da noi"*[31], si potrebbe ritenere che la singola autorizzazione resa *ad hoc* per ogni operazione coinvolga sia l'Italia come Stato sul piano della responsabilità internazionale "per complicità"[32], sia i soggetti afferenti alla catena di comando italiana coinvolta nella singola autorizzazione sul piano della responsabilità penale per ciascuno dei corrispondenti attacchi commessi all'estero: e tanto sull'assunto che la condotta prodottasi in Italia -*id est* il decollo autorizzato del drone armato- costituisce frazione antecedente necessaria della successiva frazione di azione illecita posta in essere all'estero -lo sganciamento del missile dal drone- e della stessa produzione dell'evento lesivo.

Resterebbe scoperto, e lasciato al giudizio caso per caso del giudice penale, il problema del soggetto (o dei soggetti) cui concretamente ascrivere la responsabilità e la questione del profilo soggettivo da esso (o essi) integrato: se cioè si possa far afferire l'illecito al regno del dolo, per il fatto dell'intervenuta autorizzazione all'operazione statunitense (dando quindi per note le ragioni e le motivazioni della stessa); o quello della colpa, ove si ritenga che l'autorizzazione sia intervenuta a fronte di un difetto di diligenza nella verifica dei fini del *targeted killing* americano.

5. Limiti e difficoltà di accertamento delle responsabilità penali individuali.

Il problema da ultimo evidenziato non costituisce un *proprium* dei soli casi di giurisdizione del terzo tipo, ma emerge come questione problematica in tutte le situazioni di sindacabilità penale dei *targeted killings* commessi a mezzo drone. Tema nel quale si intrecciano profili problematici di vecchio e nuovo conio: come, tra le criticità del primo tipo, l'antico ma sempre attuale tema della possibile apposizione del segreto di stato agli atti governativi che possano assumere rilevanza per l'ascrizione e l'accertamento delle responsabilità penali in materia; così, tra le difficoltà del secondo tipo, quella dell'ammissibilità anche in Italia delle richieste di accesso civico generalizzato –secondo la cd. normativa *FOIA (Freedom of Information Act)*– ai documenti in possesso delle amministrazioni pubbliche secondo le indicazioni contenute nel D.lgs. 97/2016, al pari di quanto già ampiamente realizzato negli Stati Uniti, dove oggetto di *FOIA* sono state e sono tuttora proprio le *policies* dell'amministrazione Obama e, in tempi più recenti, di quella Trump sulla gestione delle operazioni compiute a mezzo drone.

La materia dei *drone strike* è pertanto governata da segreti di Stato, da diffusi silenzi e da omessi disvelamenti di informazioni e dati sull'articolazione delle competenze per ogni attacco e da un malcelato rifiuto alla cooperazione giudiziaria ed investigativa tra Stati: situazioni che inevitabilmente incidono sulla corretta costruzione delle imputazioni, minano la completezza e correttezza delle indagini, inibiscono l'accesso delle vittime al giudice naturale come garantito sia a livello convenzionale (art. 6 par. 1 Cedu) che costituzionale (art. 25 co. 1 Cost.). Specie considerando che la stessa pratica del *targeted killing* è lesiva del diritto di ciascun soggetto ad un giusto processo e si risolve a tutti gli effetti in una uccisione *extra* e *super* giudiziale in contrasto con la pratica dei diritti umani[33].

[31] Le parole sono riportate dal sito dell'*Ansa*.
[32] Alla *complicity* sembra riferirsi l'art. 16 del Progetto sulla responsabilità degli Stati per illeciti internazionali (*Responsibility of States for Internationally Wrongful Acts*), che impiega i termini di "aiuto e assistenza", con essi riferendosi a qualsiasi tipo di condotta, comunque qualificata, che si risolva nella fornitura di assistenza militare, economica o tecnica ad uno Stato terzo ai fini della realizzazione di un illecito internazionale. Nella dottrina internazionalistica, cfr. Jackson (2015); De Wet (2018), pp. 287-313; Lanovoy (2016).
[33] Kaufman e Weiss Fagen (1981), pp. 81-100; Otto (2012), p. 3 e ss.; Farer e Bernard (2016), pp. 108-133; Ruschi (2017), pp. 45-76.

5.1. *Segreti di Stato "interni" ed "esterni".*

In prima battuta, quindi, è ammissibile, e in che misura, l'apposizione del segreto di Stato (italiano o straniero) ai contenuti delle attività di *intelligence* che, in questa materia, costituiscono parte preponderante del compendio probatorio disponibile?

Parte della dottrina ha evidenziato la controversa sovrapposizione tra "stato di emergenza" e secretazione dei dati investigativi[34], nella misura in cui si è dato atto di un tendenziale ampliamento dei casi di segreto delle attività di *intelligence*, quanto più lo Stato si trovi ad agire in contesti di emergenza a protezione della sicurezza nazionale[35]. Considerando però che l'apposizione del segreto è attività discrezionale politica[36], risultato della ponderazione del rapporto logico-strumentale tra l'attività alla quale il segreto è apposto e le finalità costituzionalmente rilevanti cui è preordinato[37], ci si chiede in che misura la scelta della secretazione sia insindacabile decisione politica o se piuttosto possa essere oggetto di valutazione in sede giurisdizionale, senza pregiudizio alla classica partizione dei poteri. In tali casi, infatti, le esigenze di verità giudiziale si scontrano con considerazioni *extra*-processuali sottese alla secretazione che, o impediscono l'identificazione dei responsabili di fatti penalmente rilevanti, o rendono ineffettive eventuali pronunce di condanna relative a soggetti già identificati, creando un profondo *gap* tra "*il lavoro degli investigatori e dei magistrati italiani, che ha permesso di identificare i responsabili e di pronunciare delle condanne nei loro confronti*"[38], e la messa in esecuzione delle condanne nel frattempo intervenute.

Per ciò che concerne il segreto di Stato "interno", la disciplina di cui alla l. 124/2007 prevede che, intervenuta la conferma *ex* artt. 41 co. 2 e 40 co. 5, l'autorità giudiziaria inibita nell'utilizzazione, anche indiretta, delle notizie segretate, ai sensi degli artt. 202, c. 5 c.p.p. e 41, c. 5 l. 124/2007, avrebbe dinanzi due strade alternative: prescindere dalla notizia se non essenziale; intervenire *pro reo*, nel caso di notizia indispensabile ai fini del decidere *ex* artt. 41 co. 3 l. 124/2007 e 202 co. 3 c.p.p., mediante declaratoria di "non doversi procedere per l'esistenza del segreto di Stato"[39]. È giocoforza che ove il Governo, come nei casi di segreto su attività di *intelligence* di attacchi a mezzo drone armato o partecipazioni in essi nei modi già riferiti, intenda bloccare l'attività giudiziaria di verifica delle responsabilità penali delle catene di comando coinvolte nell'attacco, potrà avvalersi del meccanismo del segreto[40]. Del resto alla luce della norma citata, la necessità che il giudice valuti l'essenzialità *ex ante* della conoscenza della notizia[41] costituisce un limite di non poco momento con riguardo all'accertamento delle responsabilità in questa materia: la difficoltà di pervenire ad una verifica di tal fatta è del vero strettamente connessa alla mancanza di dati certi su ordini impartiti, legittimità degli stessi, *background* di competenze ed autorizzazioni di base, verbali delle singole operazioni e verbali di dati e informative raccolte in base a verifiche preliminare ad ogni singolo attacco. Le informazioni sui singoli attacchi si fanno esse stesse contenuto delle imputazioni, per cui venendo meno le une, si smembrano a cascata le altre.

[34] Rossi Merighi (1994), p. 256.

[35] Con le sentenze C. cost. n. 82/1976 e n. 86/1977 (rispettivamente disponibili ai seguenti *link* e *link* del sito ufficiale) la Corte Costituzionale ha rintracciato nella sicurezza dello Stato-comunità l'interesse sotteso alla disciplina del segreto di stato, che la Corte nella seconda delle pronunce citate esplicitamente differenzia dall'interesse politico-governativo e partitico.

[36] Che si tratti di attività discrezionale ma non libera lo chiarisce Anzon (1976), p. 1770. Secondo l'Autrice la volontà dell'autorità competente alla qualificazione dell'attività come segreta non implica di per sé che questa "*fuori dai casi in cui si provveda con legge o con atto equiparato, possa apporne a suo arbitrio l'etichetta […]. Trattasi pur sempre di attività non libera ma discrezionale […]*". Ancora, nel caso Abu Omar (C. cost., sent. n. 106/2009, a questo *indirizzo*) la Corte specifica che: *"[…] l'individuazione dei fatti, degli atti, delle notizie, ecc. che possono compromettere la sicurezza dello Stato e devono, quindi, rimanere segreti costituisce il risultato di una valutazione ampiamente discrezionale e, più precisamente, di una discrezionalità che supera l'ambito e i limiti di una discrezionalità puramente amministrativa, in quanto tocca la salus rei pubblicae [...] atteso che il giudizio sui mezzi ritenuti necessari o soltanto utili a garantire la sicurezza dello Stato spetta al Presidente del Consiglio dei Ministri sotto il controllo del Parlamento"* (par. 12.4).

[37] La Corte Costituzionale individua il contenuto della nozione di segreto nel *"supremo interesse della sicurezza dello Stato nella sua personalità internazionale, e cioè l'interesse dello Stato-comunità alla propria integrità territoriale, alla propria indipendenza e – al limite – alla stessa sua sopravvivenza"* (C. cost.., sent. n. 82/1976; cfr. altresì sentt. n. 86/1977 e n. 110/1998).

[38] *Nasr e Ghali c. Italia* [2016] ECtHR Appl. No. 44883/09, § 272.

[39] Cfr. C. App. Milano, sez. III, 15.12.10 (dep. 15.3.11), Pres. Silocchi, Est. Manca, imp. Adler e a.; Trib. Milano, sent. n. 12428 del 4.11.2009 (Caso Abu Omar).

[40] Così la sentenza della Corte Edu sul caso Abu Omar, nella quale si afferma che l'apposizione del segreto di Stato ad opera del Governo sulla maggioranza delle fonti di prova a carico degli imputati del SISMI, trattandosi di segreto su emergenze ricadenti su circostanze di dominio pubblico, avesse come unico obiettivo quello di garantire l'impunità degli stessi. Per una lettura di sintesi delle varie tappe della vicenda si rinvia a Mariotti (2016).

[41] Setti (2015).

Cosa invece nei casi di segreto di Stato "straniero", relativo ad attività di *intelligence* compiute da altri Stati e inibite nel loro utilizzo per esigenze di *national security*? Nulla la disciplina citata prevede: si potrebbe allora sostenere che astrattamente un segreto che è tale nell'ordinamento d'origine, non potrebbe opporsi come "segreto di Stato" in un ordinamento straniero. Ragionando però *a fortiori* rispetto a quanto già osservato con riguardo al segreto "interno", si può rilevare che le ragioni sottese alla secretazione nello Stato straniero potrebbero risuonare negli stessi termini per lo Stato in cui l'atto secretato assume rilevanza. Il potere esecutivo, in altre parole, potrebbe ritenere necessario opporlo ove ritenga che la sicurezza dello Stato quale *"interesse essenziale, insopprimibile della collettività, con palese carattere di assoluta preminenza su ogni altro"*[42], passi anche attraverso il mantenimento di rapporti internazionali o il rispetto di accordi di cooperazione (realizzati mediante rispetto reciproco delle scelte assunte in sede interna dai singoli Governi), e quindi a discapito del "diritto alla verità" o all'accesso alla giurisdizione.

È in ogni caso evidente che la mancata ostensione delle informazioni ai fini della conduzione delle indagini è giustificata dal timore che la magistratura possa ingerirsi in scelte discrezionali di competenza governativa, specie se straniere; sicché opponendo la *political question doctrine*[43] e la sussistenza di esigenze di tutela della sicurezza nazionale, si finisce per ledere il "diritto alla verità" inteso come diritto al legittimo riconoscimento delle pretese vantate da quanti possano dirsi interessati, *iure proprio* o *iure hereditatis*, dagli effetti di tali scelte politiche, ma, del vero, dall'intera collettività dei cittadini la cui protezione si adduce come ragione giustificatrice degli attacchi.

5.2. *Assunti di fondo per la formulazione dell'imputazione.*

A questo punto, alla luce dello scarno compendio documentale a disposizione, si tenterà di fornire delle indicazioni di massima che si spera possano essere riempite di contenuto in un futuro non troppo remoto.

Due elementi paiono caratterizzare le ipotesi di omicidi mirati a mezzo drone di cui si discute: gli attacchi, almeno in Yemen, Somalia e Pakistan, ove la giurisprudenza per *drone strike* è più significativa, sono per lo più sferrati dalla *CIA*, organo governativo di *intelligence* e non militare[44]; le persone offese del procedimento penale sono soggetti non coinvolti nelle ostilità.

Si tratta di due assunti pericolosi, ove impiegati in senso contrario: per evitare di addentrarsi nel pantano della prova della responsabilità penale degli addetti all'operazione, e al fine di far arenare il procedimento penale con l'accoglimento della richiesta di archiviazione formulata dalla Procura, potrebbero infatti, come è invero già accaduto, adottarsi due prospettive sufficientemente vantaggiose.

Potrebbe affermarsi che la *CIA* sia *de facto* un organo militare, dipendendo comunque dal Presidente degli Stati Uniti come *Commander in Chief*, così consentendo agli agenti governativi di godere delle immunità militari e degli altri benefici legati alla qualificazione in termini di "guerra" della lotta al terrorismo. Tanto, però, non tenendo in debito conto la strutturazione interna di tale organismo e delle sue attività, entrambe prive di natura militare[45]. Tale è stata ad esempio l'impostazione assunta dall'organo di accusa nel procedimento Lo Porto e invece avversata da una pronuncia dell'Alta Corte penale di Peshawar del Pakistan[46], la quale qualifica le condotte di *targeted killings* statunitensi come crimini internazionali soggetti alle regole di *law enforcement* e agli obblighi di tutela dei diritti dei diritti umani posti a carico di ciascuno Stato.

In alternativa (o in aggiunta), si potrebbe sostenere che i soggetti contro cui l'attacco è sferrato non siano estranei al combattimento, così evitando la qualificazione del fatto omici-

[42] Cfr. la già citata C. cost., sent. n. 106/2009. Quello alla sicurezza nazionale è del resto uno degli interessi pubblici che costituiscono limite alla possibilità di accesso civico, ai sensi dell'art. 5-*bis* del D.Lgs. 33/2013, introdotto dall'art. 6, comma 2 del D.lgs. 97/2016.
[43] Per la prima volta affermata in 246 U.S. 297 (1918) (U.S. Supreme Court, Oetjen v. Central Leather Co.); cfr. Seidman (2004).
[44] Cfr. Penney, Schmitt, Callimachi e Koettl (2018); in precedenza si veda Mazzetti (2013).
[45] La distanza che intercorre tra le forze militari -combattenti legittimi- e la *CIA* è evidente ove si consideri che il personale di tale Agenzia non è chiamato a conformare la propria condotta alle leggi sui conflitti armati, non indossa uniformi, non afferisce a strutture gerarchiche esterne di tipo militare ma si inscrive in un'autonoma catena di comando interna all'Agenzia stessa (cfr. O'Connell (2013)).
[46] *Foundation for Fundamental Rights v. Federation of Pakistan et al.*, case No. 1551-P/2012, Judgment (Peshawar High Court, Pakistan, March 11, 2013).

diario come *collateral damage*. Questa impostazione è stata sposata in particolare dal Procuratore Federale della Germania nel caso, archiviato, dell'omicidio, commesso a mezzo drone armato, del cittadino tedesco Bünyamin[47]. Una soluzione che esime il giudice dall'individuare gli autori dell'operazione, ricostruirne le relative responsabilità, e dall'investigare i rapporti di collaborazione e il regime dello scambio di informazioni e dati sulle operazioni di *drone strike* tra Stati Uniti e lo Stato di volta in volta coinvolto[48].

Invero, anche ove si condividano i due assunti di base e si eserciti l'azione penale, le difficoltà si annidano sul versante dell'imputabilità, dell'antigiuridicità e della colpevolezza.

Come emerge dalla *PPG* ostesa durante la Presidenza Obama, oltre che dalle fonti innanzi citate, la decisione di operare un omicidio mirato tramite drone è il frutto di un processo interno all'organo statunitense a ciò legittimato, nella specie, il *Counter Terrorism Center* (*CTC*) della *CIA*, deputato alla raccolta e rielaborazione di *intelligence*, e a compiti operativi[49]. Dirigiamo pertanto il *focus* d'indagine all'interno della suddetta Agenzia, ed in specie proviamo a ricostruire quale sia la sua strutturazione soggettiva interna direttamente investita dal problema della responsabilità penale personale per le operazioni di *drone strike*.

5.3. *Responsabilità penali della catena di comando: brevi rilievi.*

Assumiamo[50] che la struttura interna del *CTC* direttamente coinvolta nella singola operazione ruoti attorno a tre categorie soggettive (ciascuna delle quali suscettibile di strutturarsi come mono o plurisoggettiva): alla base si collocano i soggetti deputati a "monitorare" il *target*; a livello intermedio gli agenti che "autorizzano" la singola operazione di *drone strike*; a livello superficiale coloro che la "gestiscono" materialmente, e tra costoro si situa l'"operatore", addetto al controllo e gestione dei comandi del velivolo armato[51].

Rispetto a tutti e tre i soggetti segnalati, un discorso sulla responsabilità appare di specifico interesse rispetto ai casi di *collateral damages*, in cui cioè ad essere attinto in via indiretta sia un soggetto diverso dal *target* selezionato. Rispetto alla già accennata possibilità di ritenere sussistente una responsabilità penale per il fatto stesso del *drone strike* sul bersaglio selezionato, il tema risulta nebuloso: mantenendo l'assetto attuale, per cui la pratica dei *drone strike* è legittima se compiuta sul bersaglio in virtù della logica bellica della lotta al terrorismo, la possibilità di ascrivere le condotte degli agenti *CIA* nell'alveo della responsabilità penale è ipotesi problematica. Al contrario, qualche spiraglio potrebbe aversi ove si modificasse l'assetto di base, restituendo agli Stati la legittimazione a sindacare anche sul piano penalistico le responsabilità per individuazione, autorizzazione e materiale esecuzione dell'ordine di uccisione dei soggetti presunti terroristi[52].

In questa sede si tenterà per cenni di fornire un quadro di sintesi dei possibili modi ricostruttivi delle responsabilità per *collateral damages*, nel convincimento che con i dovuti corret-

[47] Bünyamin E., cittadino tedesco, fu ucciso in Pakistan il 4 ottobre 2010 in conseguenza di un attacco armato a mezzo drone. La legge penale tedesca (§ 152 (2) StPO, § 160 StPO, § 7 (1) StGB) prevede l'attivazione di un procedimento penale in tutti i casi in cui un cittadino sia ucciso all'estero. Aperto un fascicolo contro ignoti dal procuratore federale, lo stesso è stato chiuso poco dopo, poiché secondo gli investigatori, Bünyamin voleva partecipare da combattente ai combattimenti nel nord del Pakistan: è stata pertanto esclusa la sua natura di civile e affermata quella di legittimo obiettivo militare, sì da escludere che la sua morte fosse crimine di guerra o omicidio di stato (condizioni, queste, necessarie per radicare la giurisdizione del giudice tedesco). Il decreto di archiviazione del Procuratore generale federale del 20 giugno 2013 è disponibile in tedesco a questo *indirizzo*; il comunicato stampa del procuratore generale del 1° luglio 2013 è disponibile a tale *link*.

[48] Si veda Ecchr (2013).

[49] Cfr. Fuller (2018).

[50] La strutturazione nei modi che seguiranno si fonda sia sulla riconosciuta competenza del *CTC* della *CIA* allo svolgimento di compiti operativi/autorizzatori oltre che di raccolta di dati frutto di attività di *intelligence*, come chiarito in precedenza, sia su quanto evincibile nelle richieste di rogatoria del caso Lo Porto ed in specie nell'asserzione citata alla nota 45, contenuta nelle richieste di rogatoria dell'ordinanza n. 159948/17 R.Gip, del 02.03.2018 con cui il Gip di Roma disponeva nuove indagini, ove si legge che "*la giudice ha ordinato che la rogatoria dovrà riguardare ogni aspetto del caso, con l'acquisizione di tutta la documentazione sull'operazione, sulla sorveglianza del compound prima e dopo l'attacco, sulle indagini condotte dal governo americano, inclusa l'identificazione dei presunti terroristi che gli Usa avevano preso di mira, nonché «l'individuazione di coloro che hanno coordinato il monitoraggio del compound, gestito ed autorizzato gli strike»*" (sottolineatura non originale): cfr. i siti dei quotidiani *Corriere.it*; *Palermotoday*; *Repubblica.it*.

[51] Per un'analisi più dettagliata circa la struttura interna del *CTC* si rinvia a Cucco e Mauri (2018), p. 71 e ss..

[52] Il tema palesa tutta la sua viscosità sol considerando che in ogni caso, anche ammettendo una sindacabilità penale in tali ipotesi, si ricadrebbe pur sempre nell'atavico problema di una possibile applicazione a tali soggetti della logica del "diritto penale del nemico", oggetto di dibattito in ordine alla sua ammissibilità e al modo stesso del suo configurarsi: sul tema si veda Jakobs (2006), p. 21. In senso critico Donini (2006), pp. 735-777; Ambos (2007), p. 29; cfr. per uno sguardo d'insieme Viganò (2006), p. 669.

tivi, le considerazioni svolte siano suscettibili di applicazione anche alle ipotesi di *drone strike* "puro".

Partiamo dalla responsabilità penale del "monitoratore", organo deputato al compimento delle verifiche preliminari sulle aree e sui soggetti "sensibili": si può osservare che, stante la specificità con cui i controlli vengono effettuati e il peculiare livello tecnologico degli strumenti di *intelligence* impiegati[53], il fatto che lo stesso possa incorrere in errori è ipotesi astrattamente possibile, benché in concreto di difficile verificazione. L'attività valutativa da questi compiuta si muove sul solco delle direttive tracciate da apposite *policies* (delle quali si dirà) e dai singoli protocolli operativi; poiché tali atti valgono in quanto tali, non avendo rilevanza giuridica "esterna", l'eventuale fallo del monitoratore assume una rilevanza in prima istanza interna al sistema. La sua attitudine a prodursi "a cascata" sugli altri soggetti della catena di comando, però, giustificherebbe l'ascrivibilità a questi di una responsabilità per colpa, postulata dalla scorrettezza commessa nell'elaborazione del dato, potendosi prospettare, in base al grado di incidenza causale sull'evento lesivo finale, una partecipazione alla condotta (dolosa, sebbene più raro, o colposa) degli autorizzatori.

Quanto al giudizio di accertamento della responsabilità del soggetto "autorizzatore", la peculiarità risiede anzitutto nella difficoltà di comprendere la natura, sindacabile o meno, dell'ordine da costui impartito e la sua possibile legittimità o illegittimità alla stregua dell'intero sistema nazionale e/o internazionale: è ovvio che in questo caso imprescindibile è la possibilità di accesso della magistratura alle informazioni in ordine alle modalità di conduzione degli attacchi per mezzo drone.

L'ostensione delle *policies* operative, alla quale invitava anche il Relatore delle Nazioni Unite Emmerson nel *Report* del 2013 in materia[54], è invero oggi ad un punto morto. Ad eccezione delle informazioni ufficiose provenienti da organizzazioni non governative, i dati più interessanti sono quelli contenuti nella *Presidential Policy Guidance* (*PPG*) per le operazioni della *CIA*, ostesa, con numerosi *omissis*, nel 2016 ma in vigore dal 2013[55] e oggi sostituita dal documento *Principles, Standards, and Procedures* (*PSP*), ancora non confermato come documento ufficiale ma su cui pende una specifica richiesta di *disclosure*[56].

Già la *PPG*, trovando applicazione ai casi di *"lethal and non-lethal uses of force"* impiegata *"outside areas of active hostilities"*, poneva numerosi quesiti in ordine alle modalità di svolgimento della singola operazione di *drone strike*: in esso le regole precauzionali per ogni singola operazione erano ridotte (per quanto si evince dalle parti non soggette ad *omissis*) essenzialmente alla verifica preliminare dell'identità del *target*, impiegando "*all reasonably available resources*", adottando "*harmonized policies and procedures*" allo scopo ultimo di affermare con "*near certainty that noncombatant will not be injured or killed*" (si veda Sezione 1. E. n. 2). Tanto però era certamente sufficiente per affermare che quella di eventi collaterali fosse ipotesi di marginale verificazione, essendo previste *policies* per evitare il prodursi di eventi collaterali *"near certainty"*, e che conseguentemente, la realizzazione degli stessi non fosse facilmente configurabile in termini di errore derivante da colpa.

Le attuali e non ostese *PSP* compiono un salto avanti nella logica protezionistica degli agenti di *CTC* competenti in tema di *drone strike*, aprendo due ulteriori squarci alla prospettiva di de-responsabilizzazione: non si intende più come condizione sottesa all'attacco che il *target* sia *"continuing, imminent threat"* e si attribuisce alla *CIA* un'autonomia estesa, eliminando l'intermediazione dell'autorizzazione del governo centrale[57].

Questa apertura sposta in avanti il confine della non punibilità, ammettendosi attacchi indiscriminati e scriminati anche a prescindere dall'effettiva conoscenza o previsione di possibili futuri attentati lesivi della sicurezza degli Stati Uniti[58], creando problemi anche rispetto al

[53] Tung (2015), p. 638.
[54] Emmerson (2014).
[55] La *PPG* dell'amministrazione Obama è oggi a disposizione e facilmente accessibile al seguente *link*.
[56] È del 21.12.2017 il *FOIA* relativo alle *policies* del Presidente Trump presentato dall'*American Civil Liberties Union* e dall'*American Civil Liberties Union Foundation*, sulla quale si veda il sito *Courthousenews.com*.
[57] Cfr. Savage e Schmitt (2017).
[58] Ad esempio, nel caso *McCann e altri v. Uk* ([1995] ECtHR Application No.18984/91), uno dei motivi di ricorso alla Corte Edu, peraltro accolto dallo stesso giudice, è centrato sulla sussistenza di difetti di pianificazione e controllo, ed in specie sulla considerazione secondo cui il fatto che i presunti terroristi avessero piazzato la bomba e che sarebbe stato per loro possibile farla esplodere in qualsiasi momento e in qualsiasi luogo, nel momento in cui fossero stati fermati, fosse una mera supposizione. La stessa Corte, infatti, usa i concetti di prudenza e attenzione nell'uso della forza contro presunti terroristi, imponendo la necessità che il sospetto sia sorretto da un *quid pluris* di informazioni e dati oggetto di valutazione: *"Their reflex action in this vital respect lacks the degree of caution in the use of firearms to be expected from law enforcement personnel in a democratic society, even when dealing with dangerous terrorist suspects, and stands in marked*

coinvolgimento degli Stati terzi che forniscano assistenza per tali operazioni: a costoro, infatti, al fine di andare esenti da responsabilità per complicità ai sensi dell'art. 16 o degli artt. 40 e 41 del *Responsibility of States for Internationally Wrongful Acts* già citato, sarà richiesto di indagare le specifiche intenzioni sottese ad ogni operazione da parte degli Stati Uniti, rinunciando a generici accordi di assistenza.

Si presume pertanto che in tale modo gli agenti abbiano un maggior margine di manovra nella scelta delle pratiche antiterrorismo più efficaci, con un'anticipazione dell'intervento certamente discutibile perché foriero di de-responsabilizzazione. Viene in questo modo a cadere, infatti, uno dei possibili pilastri dell'impianto difensivo, fondato sulla contestazione della ragionevolezza dell'attacco, introducendosi una sorta di presunzione assoluta di ponderatezza della decisione sulla scorta di un mero sospetto di minaccia e non di minaccia vera e propria di attacchi terroristici.

È chiaro che a questo punto diventa centrale il problema se un ordine, che sia legittimo[59] per il sistema in cui si incasella il funzionario che lo emette, possa però essere illegittimo nella prospettiva della tutela dei diritti umani delle vittime collaterali dell'attacco e a questo punto, con le *PSP*, anche dei *target* designati; e se, conseguentemente, tanto incida anche sull'accertamento della responsabilità, con contestazione a catena dell'ammissibilità delle *PSP* stesse (e prima di queste della *PPG*) e delle *policies* e *procedures* che ne costituiscono attuazione, in una prospettiva di diritto internazionale dei diritti umani. Inoltre, l'individuazione dell'ordine come illegittimo potrebbe aprire le porte ad una sostanziale non antigiuridicità della condotta dell'operatore, nei cui confronti si giustificherebbe l'applicazione della scriminante *ex* art. 51 c.p., ove si considerasse l'ordine come insindacabile.

PSP e *PPG* sono però utili anche nella misura in cui facilitano l'individuazione dell'elemento soggettivo dell'autorizzatore. Si legge nel secondo di tali documenti che gli attacchi devono essere frutto di valutazioni dettagliate e si descrive il drone come strumento "notevolmente preciso e limitato in termini di danni collaterali": tradotto, ogni effetto collaterale, vista la precisione dello strumento, è previsto in misura assoluta o comunque notevolmente elevata. Questo indurrebbe l'esclusione di qualsiasi profilo di colpa, anche con previsione, rispetto al caso in cui l'attacco attinga soggetti diversi dai *target* selezionati, emergendo l'esistenza di una volontà di agire in vista dell'obiettivo, appunto voluto, dell'uccisione mirata; anche perché alla luce delle statistiche sui *collateral damages*, ove si affermasse la colpa, la frequenza degli errori dovrebbe indurre quantomeno ad un ripensamento della validità delle procedure applicate: alla data in cui si scrive, infatti, su 6.786 *strikes* confermati e su un totale di uccisi tra 8.459 e 12.105 soggetti, si contano tra 769 e 1.725 vittime non consentite[60].

Imponendosi pur sempre un'analisi *case by case* degli indicatori fattuali del dolo (natura e modalità di svolgimento della condotta, luogo, durata ed eventuale reiterazione della stessa, comportamenti precedenti, dati e documenti a disposizione dell'agente, qualifica, contesto lecito o illecito di base, finalità della condotta e compatibilità con l'evento collaterale)[61], è astrattamente intuibile come sia superata la soglia della mera prevedibilità e non accettazione dell'evento morte della vittima collaterale a tutto vantaggio di quella integrante le forme di dolo diretto o eventuale[62]. Così potrebbe sostenersi che l'autorizzazione sottendesse l'intenzione specifica e diretta di far saltare in aria il *compound* ove si trovava il *target* terroristico di

contrast to the standard of care reflected in the instructions in the use of firearms by the police which had been drawn to their attention and which emphasised the legal responsibilities of the individual officer in the light of conditions prevailing at the moment of engagement (see paragraphs 136 and 137 above). This failure by the authorities also suggests a lack of appropriate care in the control and organisation of the arrest operation", sul sito della *Cedu*.

[59] La legittimità è qui intesa in senso formale, e riferita ad un ordine emesso in seno ad un rapporto di diritto pubblico, ad opera di un'autorità competente, nel rispetto delle forme prescritte ed il cui contenuto sia compatibile con gli incarichi propri di chi lo esegue "*quanto all'essenza, ai mezzi ed al fine*": cfr. Cass. pen, Sez. 1, sent. n. 4194 del 27 gennaio 1987; Cass. pen, Sez. 1, sent. n. 11159 del 10 giugno 1982.

[60] Si tratta di dati forniti dal *database* del *The Bureau Investigative Journalism*, disponibili a questo *link* (consultati l'ultima volta in data 27.09.2019).

[61] Per una lettura analitica dell'operare dei citati indicatori, si rinvia a Cucco e Mauri (2018) pp. 79-83.

[62] Cass. pen., Sez.1, sent. n. 12954 del 29 gennaio 2008; cfr. altresì Dova (2015), p. 13, che riporta e traduce quanto affermato da BGH, 28 febbraio 2013-4 StR 357/12, in *Neue Zeitschrift für Strafrecht*, 2013, p. 538 ss., secondo cui, *"(…) in caso di condotte violente estremamente pericolose, è evidente che il reo fa i conti con la possibilità che la vittima possa morire e – poiché egli nondimeno prosegue nella sua azione – mette in conto un tale evento. Per questo motivo, in tali casi, è di massima possibile trarre la conclusione che sussista il dolo eventuale, in ragione dell'obiettiva pericolosità della condotta del reo. A questo scopo c'è bisogno di una visione d'insieme di tutte la circostanze di fatto oggettive e soggettive del caso di specie, tra le quali sono soprattutto da includere l'oggettiva pericolosità della condotta, le modalità concrete di aggressione da parte del reo, le sue condizioni psichiche al momento della commissione del fatto e i suoi motivi*"; ancora, nella letteratura straniera, si veda Ohlin (2013), pp. 79-130.

riferimento, e che la morte dei *target* non consentiti ivi presenti (certamente previsti alla luce della precisione della tecnologia del drone e delle informazioni dettagliate raccolte dall'*intelligence*) sia proprio il mezzo al fine caratteristico dell'intenzione diretta e prefigurato come probabile (dolo diretto); oppure che sia soltanto un rischio accettato, che si verifica pertanto come sopportata conseguenza, prevista in termini di possibilità, dell'azione diretta ad altro fine (dolo eventuale).

Collegata alla responsabilità di cui sopra è quella relativa all'ultimo dei soggetti della catena, chiamato ad eseguire materialmente gli ordini impartiti mediante la gestione diretta e da remoto del drone. Quasi come il giocatore di un *videogame* con in mano il suo innocuo *joystick*, il giocatore della "guerra del terrore" assume il compito di condurre in modo diretto l'operazione, attraverso la predisposizione del piano di volo del drone, la gestione diretta dei comandi, l'impostazione e il posizionamento del mirino dei missili e il loro rilascio sul *target*[63]. Che tipo di responsabilità imputare a tale soggetto nel caso in cui la sua condotta sia produttiva dell'evento lesivo non solo ai danni del bersaglio terroristico, ma vieppiù di un *target* non selezionato?

Tale accertamento interroga l'interprete sul versante dell'antigiuridicità prima ancora che su quello della colpevolezza. Mentre è certamente integrata la tipicità del fatto, coincidente con la morte della vittima non designata, le altre due dimensioni del reato, avvinte da un nesso di consequenzialità, appaiono di non agevole identificazione. Pur nella consapevolezza della relatività di tutte le considerazioni spendibili sul tema, è certo che un discorso sulla non antigiuridicità della condotta dell'operatore materiale ruota attorno all'identificazione della natura dell'ordine ricevuto dal soggetto a lui sovraordinato (innanzi identificato nell'autorizzatore) e nel maggiore o minore grado di discrezionalità nella sua esecuzione, e risulta preliminare a qualsiasi analisi sulla dimensione soggettiva del fatto.

Come già riferito, l'operatore nell'attivazione da remoto dei comandi del drone, agisce secondo le coordinate dettate a livello sovraordinato. Due le situazioni verificabili: a) la presenza delle vittime collaterali non è nota, o è nota ma non è comunicata all'operatore; b) l'autorizzatore è consapevole della possibile presenza *in loco* di soggetti non-*target*, e dell'attitudine dell'attacco ad attingerli in uno con le vittime terroristiche designate, e nonostante ciò impartisce l'ordine, fornendo il quadro di riferimento anche all'operatore.

La prima situazione fattuale non sembra di frequente verificazione: alla luce delle indicazioni di cui alla *PPG*[64] e come già rilevato con riguardo al monitoratore, anche rispetto a questa ipotesi non pare peregrino il convincimento secondo cui nella prassi l'operazione è condotta con il possesso di conoscenze e dati in numero significativo e l'ordine di attacco postula la piena consapevolezza del contesto fattuale in cui esso è sferrato. Così si può sostenere che l'operatore riceva le informazioni necessarie per condurre il *drone strike* nei limiti di quanto necessario per il contenimento del rischio terroristico, rispondendo anch'egli al vincolo di cui alla *PPG* di adottare" "*harmonized policies and procedures*" perché si abbia la "*near certainty that noncombatants will not be injured or killed*" (Sez. 1.E. n. 2).

Passiamo alla seconda situazione: esiste e, in caso positivo, qual è l'estensione della capacità dell'operatore di sindacare la (il)legittimità dell'ordine ricevuto? Nessuna indicazione è possibile rinvenire nella *PPG*[65]: pertanto, sebbene la meccanicità dell'attività compiuta da tale soggetto[66] induca a ritenere che egli non sia legittimato a compiere alcuna valutazione, in verità lo stesso non varrebbe ove il superiore gerarchico desse l'ordine specifico di attaccare un *target* non consentito[67].

Sicché, fuori da tale ultima ipotesi, verrebbe in rilievo la possibile scriminabilità della condotta dell'operatore *ex* art. 51 co. 4 c.p.[68]. È chiaro che sposando tale assunto l'operatore

[63] Dà conto in modo drammatico e quasi romanzesco di tale asettica attività cfr. Langewiesche (2011), p. 77 e ss..
[64] Si legge già in apertura che *"Any direct action must be conducted lawfully and taken against lawful targets; wherever possible such action will be done pursuant to* -omissis- *a plan*".
[65] Di competenze a sindacare la legittimità dell'ordine dell'autorizzatore da parte dell'operatore, non è dato rintracciare indicazioni nella *PPG*, dove tra la Sezione 5 in tema di "*Procedures for Approving Proposals that Vary from the Policy Guidance Othenvise Set Forth in this PPG*" (p. 16) e la sezione 6 "*Procedures for After Action Reports*", si nota l'assenza del momento critico del *drone strike* vero e proprio.
[66] Che l'attività dell'operatore risulti prevalentemente "robotica" ed "esecutiva" è confermata dalle dichiarazioni rilasciate da *ex servicemen* statunitensi, come risultanti da interviste o testi letterari: si veda, tra gli altri, Langewiesche (2011); o le parole spese da Cian Westmoreland e Lisa Ling (le cui interviste sono riportate sui siti dei giornali *Theguardian.com* e *Aljazeera.com*).
[67] Cfr. Cass. pen., Sez. 5, sent. n. 38085 del 05 luglio 2012; Cass. pen, Sez. 5, sent. n. 16703 del 11 dicembre 2008; sulla sindacabilità dell'ordine illegittimo nelle gerarchie delle forze armate e di polizia cfr. Cass. pen., Sez. 6, sent. n. 178 del 28 settembre 1984.
[68] Invero, parte della dottrina ritiene che in tale ipotesi la mancata configurazione del fatto si avrebbe in punto di colpevolezza, poiché la libertà dell'agente risulterebbe coartata da una pressione psicologica legata al rapporto gerarchico: così Fiandaca-Musco (2019), p. 432.

resterebbe indenne da responsabilità; e a monte l'autorizzatore, la cui decisione si legittimi nell'ordinamento delineato dalla *PPG*. Restando così il diritto penale escluso dal campo del *drone strike*, con buona pace di quanti sostengono, come si fa in questa sede, l'illegittimità della *Global War on Terror* e la sua afferenza all'area del *IHL*.

Lo scenario cambia, però, modificando il parametro di riferimento: ammettendo la sindacabilità della PPG in una prospettiva internazionale, la sindacabilità dell'ordine diventa possibilità e invita a ripensare la scriminabilità della condotta dell'operatore ex art. 51 co. 4 c.p. nel caso in cui l'ordine fosse illegittimo e non sia stato censurato, esclusa la possibilità di errori circa la sua natura (art. 51 co. 3 c.p.), e fatta salva la responsabilità dell'autorizzatore ai sensi del co. 2 della medesima norma. Ne seguirebbe la possibilità di contestare un'imputazione per omicidio volontario in concorso *ex* artt. 110-575 c.p., con l'attenuante, per l'operatore, prevista al combinato disposto degli artt. 114 co. 3 e 112 co. 1 n. 3 c.p..

Diversamente, nel caso in cui si ritengano le regole della *PPG* non sindacabili e si assuma come legittimo l'ordine impartito, l'analisi dell'interprete dovrà assestarsi sul piano della colpevolezza, verificando la dimensione dolosa o colposa della condotta esecutiva dell'operatore ove, nel primo caso, essa sia volontariamente produttiva dell'evento collaterale in spregio dell'ordine ricevuto, invece attento ad evitare il prodursi di danno "fuori *target*"[69], oppure ove egli abbia agito con negligenza o imprudenza esecutiva[70].

6. Conclusioni.

Insomma, in materia di *targeted killings* a mezzo droni armati, "l'uomo a terra" muoverebbe la leva salvando i cinque soggetti legati alle rotaie ma uccidendo l'unico legato al secondo binario, e "l'uomo magro" spingerebbe giù dal ponte quello grasso per fermare il treno: la decisione per l'azione è però ponderata e consapevole. L'inevitabilità dell'evento e la fatalità della situazione sono create artificialmente dall'agente, che le adotta come giustificazioni posticce ad una scelta uno contro cinque motivata da esigenze di sicurezza nazionale ed internazionale[71]. Potrebbe quindi il diritto penale punire "l'uomo a terra" e "l'uomo magro", prescindendo dalle motivazioni nobili di cui gli stessi si sono fatti portatori nel porre in essere la condotta?

Nel *drone strike* l'"uomo a terra" e l'"uomo magro" sono però figure plurisoggettive: certamente in esse vi rientrano l'autorizzatore e l'operatore, e di quest'ultimo, in specie, l'azione lesiva è intermediata da un'arma che crea una distanza fisica ed emotiva con le vittime, riducendo la percezione della dannosità della condotta consistente nel decidere l'attacco e manovrare il *joystick* (un po' come accade nel caso dell'uomo a terra che spinge la leva, e la cui condotta lesiva è indirettamente produttiva dell'evento collaterale alle vittime non designate); ma per di più la condotta è sostenuta dal convincimento circa la bontà dell'atto, come giustificato nella prospettiva della *Global War on Terror* da esigenze di tutela della sicurezza nazionale ed internazionale, al punto da ritenere sostenibili gli eventuali danni collaterali[72]. Ed allora, si potrebbe affermare che gli stessi Stati che ricorrono al drone come arma semi-autonoma per attuare politiche di *counterterrorism* siano fautori della scelta di agire "anche a costo di". Accanto però ad una responsabilità di tipo internazionale, la necessità di ricorrere allo strumento penale si giustifica in ragione della personale, colpevole e antigiuridica condotta della catena di comando coinvolta nell'operazione. Escludere l'operare del diritto penale adducendo motivazioni legate a strategie antiterrorismo è un modo di de-responsabilizzare soggetti che gestiscono armi di grande impatto e di pericolosità massima, stante la separazione sul piano psichico, oltre che fisico, che determinano tra vittima e autore.

"L'uomo a terra" e "l'uomo magro" vanno pertanto puniti? La risposta che astrattamente dovrebbe darsi, alla luce delle considerazioni innanzi spese, pare essere positiva sebbene, come si è avuto modo di notare, gli elementi per accertare in concreto le responsabilità e per evitare una (facile) archiviazione scontano il limite della segretezza delle informazioni di Stato, dell'occultamento dei dati relativi alle operazioni già compiute, del diniego di cooperazione tra Stati per la costruzione di capi di imputazione su soggetti determinati.

[69] Cass. pen, Sez. 4, sent. n. 53150 del 28 settembre 2017; Cass, pen., Sez. 1, sent. n. 20123 del 20 gennaio 2011.
[70] Trinchera (2011).
[71] Sull'attribuzione di competenze in materia alla *CIA* e l'ampiamento delle stesse in casi di minaccia alla sicurezza nazionale provenienti da individui, si veda Banks (2015), pp. 129-159.
[72] Meloni (2016), pp. 47-63.

Il diritto penale non può tuttavia rinunciare ad intervenire: lo chiedono le vittime sacrificate per "presunte giuste cause"; lo chiede la comunità internazionale, come argine al rischio di un'espansione incontrollata di decisioni di uccisioni mirate, già sindacabili di per sé, e vieppiù critiche se produttive di eventi collaterali come "costi sopportabili" in base a valutazioni acritiche. Perché non è detto che in tale caso il "treno del terrore" sia realmente fuori controllo e la morte collaterale sia necessariamente ineluttabile: la consapevolezza sottesa alla decisione di agire "anche a costo di" ha un peso, e il diritto penale è chiamato a quantificarlo, perché la scelta volontaria di uccidere uno per salvarne cinque non sia assunta a cuor leggero.

Bibliografia

Ambos, Kai (2007), "Il diritto penale del nemico", in Donini, Massimo – Papa, Michele (editors), *Diritto penale del nemico. Un dibattito internazionale*, (Milano, Giuffrè), pp. 29-64

Anzon, Adele (1976): "Segreto di Stato e Costituzione", *Giurisprudenza Costituzionale*, I, 2, pp. 1755-1799

Banks, William C. (2015): "Regulating Drones. Are Targeted Killings by Drones Outside Traditional Battlefields Legal?", in Bergen, Peter L. e Rothenberg, Daniel (editors), *Drone Wars. Transforming Conflict, Law, and Policy*, (Cambridge, Cambridge University Press), pp. 129-159

Berto, Lucrezia (2017): "La responsabilità civile dei robot: dalla Risoluzione del Parlamento Europeo all'articolo 2043 c.c.", *IusinItinere*

Bin, Roberto (2007): "Democrazia e terrorismo", in De Maglie, Cristina e Seminara, Sergio (editors): *Terrorismo internazionale e diritto penale* (Padova, Cedam), pp. 39-54

Cerqua, Luigi Domenico (2007): "Sulla nozione di terrorismo internazionale", *Cassazione penale*, p. 1578

Cucco, Carla e Mauri, Diego (2018): "Omicidi mirati a mezzo drone: brevi riflessioni a margine del caso "Lo Porto" tra diritto penale e diritto internazionale", *Diritto penale contemporaneo*, 5, pp. 65-90

De Vergottini, Giuseppe (2004): "La difficile convivenza tra libertà e sicurezza. La risposta delle democrazie al terrorismo. Gli ordinamenti nazionali", *Boletin Mexicano de Derecho Comparado*, 37, pp. 1185-1211

De Wet, Erika (2018): "Complicity in the Violations of Human Rights and Humanitarian Law by Incumbent Governments Through Direct Military Assistance on Request", *International and Comparative Law Quarterly*, 67, 2, pp. 287-313

Della Morte, Gabriele (2009): "Sulla giurisprudenza italiana in tema di terrorismo internazionale", *Rivista di Diritto Internazionale*, XCII, 2, p. 443-475

Di Stasio, Chiara (2010): *La lotta multilivello al terrorismo internazionale. Garanzia di sicurezza versus tutela dei diritti fondamentali*, (Milano, Giuffrè)

Donini, Massimo (2006): "Il diritto penale di fronte al "nemico"", *Cassazione penale*, pp. 735-777

Dova, Massimiliano (2015): "*Un dialogo immaginario con la giurisprudenza tedesca sui confini del dolo. In tema di omicidio e "soglia d'inibizione"*", *Diritto penale contemporaneo – Rivista Trimestrale*, 4, pp. 368-384

Ecchr (2013): *Targeted Killing by Combact Drone. Expert opinion on the decision (File no. 3 BJs 7/12-4) of the Federal Prosecutor General at the Federal Court of Justice to discontinue investigatory proceedings into the killing of German national Bünyamin E. on 4 October 2010 in Mir Ali / Pakistan*, *StateWatch.org*

Emmerson, Ben (2014): *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, A/HRC/25/59, *Ohchr.org*

Farer, Tom e Bernard, Frederic (2016): "Killing by Drone: Towards Uneasy Reconciliation with the Values of a Liberal State", *Human Rights Quarterly*, 38, pp.108-133

Fiandaca, Giovanni e Musco, Enzo (2019): *Diritto penale. Parte generale*, VIII (Bologna, Zanichelli)

Foot, Philippa (1967): "The Problem of Abortion and the Doctrine of Double Effect", *Oxford Review N. 5*, *Philpapers.org*, pp. 5-15

Fuller, Christopher J. (2018): "The Origins of the Drone Program", *LawFare Blog*

Greene, Joshua (2007): "The Secret Joke of Kant's Soul", in Sinnott-Armstrong, Walter, (editor): *Moral Psychology. Volume 3. The Neuroscience of Morality: Emotion, Brain Disorders, and Development*, (Cambridge, MIT Press), pp. 35-80

Hallevy, Gabriel (2010): "The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control", *Akron Intellectual Property Journal*, 4, 2, 1, p. 171-201

Istituto Di Ricerche Internazionali Archivio Disarmo - Iriad, (2017): *Droni Militari: Proliferazione o controllo?*, Sistema Informativo a Schede (SIS), Rapporto di ricerca (Roma), *IRIAD*

Jackson, Miles (2015): *Complicity in International Law*, (Oxford University Press)

Jakobs, Günther (2006): "Derecho penal del ciudadano y derecho penal del enemigo", in Jakobs, Günther e Cancio Meliá, Manuel (editors), *Derecho penal del enemigo* (Madrid, Cuadernos Civitas), pp. 21-56

Kaufman, Edy e Weiss Fagen, Patricia (1981): "Extrajudicial Executions: an Insight into a Global Dimensions of a Human Rights Violation", *Human Rights Quarterly*, 3, pp. 81-100

Koh, Harold Hongju (2010): *The Obama Administration and International Law. Keynote Speech at the Annual Meeting of the American Society of International Law* (speech at Annual Meeting of the American Society of International Law), *U.S. Department of State*

Langewiesche, William (2011): *Esecuzioni a distanza* (Milano, Adelphi)

Lanovoy, Vladyslav (2016): *Complicity and its Limits in the Law of International Responsibility*, (Oxford, Hart Publishing)

Lubell, Noam (2012), "The War (?) against Al-Qaeda", in Wilmshurst, Elizabeth (editor), *International Law and the Classification of Conflicts* (Oxford, Oxford University Press), *SSRN*, pp. 421-454

Lubell, Noam e Dereiko, Nathan (2013): "A Global Battlefield?: Drones and the Geographical Scope of Armed Conflict", *Journal of International Criminal Justice*, 11, 1, pp. 65–88

Lubold, Gordon e Barnes, Julian E. (2016): "Italy Quietly Agrees to Armed U.S. Drone Missions Over Libya", *The Wall Street Journal*

Mariotti, Marco (2016): "*La condanna della Corte di Strasburgo contro l'Italia sul caso Abu Omar. Corte Edu, IV sezione, Nasr e Ghali c. Italia*, sent. 23 febbraio 2016 (ric. n. 44883/09)", *Diritto penale contemporaneo*

Mauri, Diego (2016): "Droni a Sigonella: quale valore ha (e quale impatto produrrà) l'accordo italo-americano", *Quaderni di SIDIBlog*, 3, pp. 319-325

Mazzetti, Mark (2013): "A Secret Deal on Drones, Sealed in Blood. Rise of the Predators", *The New York Times*

Meloni, Chantal (2016): "State and Individual Responsibility for Targeted Killings by Drones", in Di Nucci, Ezio e Santoni de Sio, Filippo (editors): *Drones and Responsibility: Legal, Philosophical, and Socio-Technical Perspectives on Remotely Controlled Weapons*, (New York, Routledge), pp. 47-63

Meloni, Chantal (2017): "Sulla (il)legittimità degli omicidi mirati mediante i droni e i possibili ricorsi alle corti", Istituto Di Ricerche Internazionali Archivio Disarmo – Iriad: *Droni Militari: Proliferazione o controllo?*, Sistema Informativo a Schede (SIS), Rapporto di ricerca (Roma), *ECCHR*, pp. 145-148

Melzel, Nils (2008): *Targeted Killing in International Law* (Oxford University Press)

O'connell, Mary Ellen (2013): "Spy vs. Soldier. The CIA may lose a power it never legally had", *The New Republic*

Ohlin, Jens David (2013): "Targeting and the Concept of Intent", *Michigan Journal of International Law*, 35, 1, pp. 79-130

Oliveri Del Castillo, Roberto (2005): "Lotta al terrorismo: garanzie e rischio se si amplia il concetto di fatto notorio", *Diritto e Giustizia*, 20, pp. 77-79

Otto, Roland (2012): *Targeted Killings and International Law: With Special Regard to Human Rights and International Humanitarian Law* (Berlino, Springer)

Penney, Joe, Schmitt, Eric, Callimachi, Rukmini e Koettl, Christoph, (2018): "C.I.A. Drone Mission, Curtailed by Obama, Is Expanded in Africa Under Trump", *The New York Times*

Pike, John (2011): "The Samsung Techwin SGR-A1 Sentry Guard Robot", *GlobalSecurity.org*

Rossi Merighi, Ugo (1994): *Segreto di Stato: tra politica e amministrazione*, Napoli, 1994

Ruschi, Filippo (2017): *El Derecho, la guerra y la "tecnica desatada": consideraciones acerca del drone warfare*, in Campione, Roger e Ruschi, Filippo (editors): *Guerra, derecho y seguridad en las relations internationales* (Valencia, Tirant lo Blanch), pp. 45-76

Savage, Charlie e Schmitt, Eric (2017), "Trump Poised to Drop Some Limits on Drone Strikes and Commando Raids", *The New York Times*

Seidman, Louis Michael (2004): "The Secret Life Of The Political Question Doctrine", *37 J. Marshall Law Review*, *Georgetown Law Faculty Publications and Other Works*, pp. 441-480

Setti, Saverio (2015): "La tutela del segreto di Stato nella procedura penale", *Sistema di informazione per la sicurezza della Repubblica*

Siciliano, Domenico (2008): "L'abbattimento di aerei civili per contrastare atti terroristici e il diritto (La situazione italiana e quella della Repubblica federale tedesca)", *Questione giustizia*, 4, pp. 173-176

The UK Approach to Unmanned Aircraft Systems (2011), Joint Doctrine Note (JDN) 2/11 (Development, Concepts and Doctrine Centre (DCDC) – Ministry of Defence UK)

Thomson, Judith Jarvis (1985): "The Trolley Problem", *The Yale Law Journal*, 94, 6, pp. 1395-1415

Tramontana, Enzamaria (2018): "Uccisioni mirate, legittima difesa preventiva e diritti umani", *Diritti Umani e Diritto Internazionale*, 12, 1, pp. 53-75

Trinchera, Tommaso (2011): "La Cassazione sulla strage di Nassiryah: l'adempimento dell'ordine del superiore non giustifica l'omesso impedimento dell'evento per negligenza o imprudenza. Nota a Cass. pen., Sez. I, sent. 20 gennaio 2011 (dep. 20 maggio 2011), n. 20123, Pres. Chieffi, Rel. Zampetti", *Diritto penale Contemporaneo*

Tung, Yin (2015): "Game of Drones: Defending against Drone Terrorism", *2 Texas A&M Law Review,* pp. 635-673

Unmanned Aircraft Systems (2017), Joint Doctrine Publication (JDP) 0-30.2 (Development, Concepts and Doctrine Centre (DCDC) – Ministry of Defence UK)

Velez-Green, Alexander (2015): "The South Korean Sentry - A "Killer Robot" to Prevent War", *LawFare Blog*

Viganò, Francesco (2006): "*Terrorismo, guerra e sistema penale*", *Rivista italiana di diritto e procedura penale*, pp. 648-703

Viganò, Francesco (2007): "Terrorismo di matrice islamico fondamentalista e art. 270-bis nella recente esperienza giurisprudenziale", *Cassazione penale*, pp. 3953-3987

Weinberger, Sharon (2014): "Next generation robots have minds of their own", *BBC*

Profili penalistici delle *self-driving cars*

Cuestiones de derecho penal en relación a los vehículos de conducción autónoma

Self-driving Cars and Criminal Law

Alberto Cappellini
Dottorando presso l'Università di Firenze
alberto.cappellini@unifi.it

Principio di precauzione, Colpa, Reati stradali

Principio de precaución, Culpa, Delitos de tránsito

Precautionary principle, Negligence, Traffic Offences

Abstracts

Lo sviluppo dell'*autonomous driving* sta compiendo passi da gigante in altri paesi e recentemente ha toccato anche l'Italia. Il presente lavoro mira a fornire un quadro generale dei possibili futuri profili di intersezione tra tale tematica e il diritto penale.

El presente trabajo tiene como objetivo proporcionar una visión general de las posibles futuras cuestiones de intersección entre los vehículos de conducción autónoma y el derecho penal.

Autonomous driving is and increasing phenomenon in several countries and recently it has involved Italy too. This paper aims to provide a general picture of the potential future intersections between the said phenomenon and the criminal law.

Sommario

1. Introduzione.

Di tutte le tecnologie legate alla robotica e all'intelligenza artificiale in corso di sviluppo negli ultimi anni, senza dubbio quella delle auto a guida autonoma è una delle più promettenti, nonché gravide di conseguenze sociali, economiche e – inevitabilmente – anche giuridiche.

In effetti, i progetti di ricerca e sviluppo avviati in materia sono moltissimi, al punto da essere difficilmente quantificabili. *CB Insight*, nel settembre 2018, contava ben 46 *corporations* al lavoro su tali tecnologie[1]. Numeri che vanno ben oltre, dunque, la ristretta cerchia dei progetti più noti al grande pubblico – *Google car* (ora *Waymo*), oppure quelli sviluppati da *Uber* e da *Tesla* – che pure probabilmente ne rappresentano la "punta" più avanzata[2].

Fino ad oggi, la sperimentazione su strada è rimasta perlopiù confinata a paesi esteri, Stati uniti *in primis*. Già dal 2014, vari stati USA – a partire dal Nevada – hanno varato regole volte a consentire la circolazione di veicoli a guida autonoma, pur assistita da precauzioni, tra cui la necessaria presenza di un collaudatore-pilota in grado di riprendere, in qualunque momento, il controllo del mezzo[3]. Dal 1° novembre 2018 la California si è spinta ancora oltre, permettendo, per la prima volta, la sperimentazione nel traffico di veicoli *Google* completamente *driverless*[4].

In Italia, solo in tempi recentissimi sono stati avviati i primi test su strada. Il decreto del Ministero delle infrastrutture e dei trasporti del 28 febbraio 2018 (c.d. *smart road*) ha infatti previsto che le aziende costruttrici, gli istituti universitari e gli enti di ricerca interessati a sperimentare i loro prototipi nel traffico possano richiedere, allo scopo, un'apposita autorizzazione ministeriale[5]. Tuttavia, ad oggi è stato rilasciato uno solo di questi permessi, giacché un'unica società ha presentato domanda per ottenerlo. Le prime auto a guida autonoma dell'azienda in questione – sempre sorvegliate da un collaudatore-pilota a bordo – hanno iniziato a circolare nel maggio del 2019, prima a Parma e poi a Torino[6].

Per il resto, all'infuori di tali regimi autorizzatori speciali, la circolazione di mezzi condotti da intelligenze artificiali è da intendersi implicitamente vietata dal Codice della strada. Ogni auto deve essere condotta da un soggetto umano che si assuma il ruolo e le responsabilità di guida: al di fuori di questo paradigma, si verte attualmente in un'area di rischio non consentito.

Quali ripercussioni comporterà, nel campo del diritto penale, l'introduzione piena e la diffusione dell'*autonomous driving*? Se la letteratura italiana ha già iniziato a interrogarsi sulle conseguenze in chiave risarcitoria connesse alla responsabilità civile[7], obiettivo di questo lavoro è invece quello di tentare di tracciare un quadro sommario dei futuri riflessi penalistici di queste tecnologie[8].

[1] CB Insight (2018). Si tratta di una importante azienda di *analytics* che opera principalmente nel settore dell'industria tecnologica.

[2] LoRicco (2018), pp. 299 ss.

[3] Wing (2016), pp. 719 ss.

[4] Waymo (2018).

[5] Delle Cave (2019). Il citato decreto è stato emanato in attuazione della legge di bilancio 2018, la quale ha stanziato due milioni di euro, per il biennio 2019-2020, proprio per incentivare le sperimentazioni relative all'*autonomous driving* e alle *smart roads* (ovvero infrastrutture stradali capaci di "dialogare" con le vetture "intelligenti"): v. Scagliarini (2018).

[6] La Stampa (2019).

[7] Per tutti, Pardolesi e Davola (2017).

[8] Non esiste ancora, a quanto ci è noto, letteratura in italiano dedicata specificamente al tema. Molto più sviluppata è invece la letteratura statunitense (e in parte anche tedesca). Come lavori generali di riferimento si possono citare fin d'ora: Douma e Palodichuk (2012), Gurney (2015), Tranter (2016), Gless (2016), Gless *et al.* (2016), Westbrook C.

Nel fare ciò, il discorso si articolerà su quattro nodi tematici fondamentali. Una prima parte dello scritto (§§ 2-3) sarà dedicata ad approfondire alcune nozioni di carattere generale riguardanti la guida autonoma. In una materia così innovativa, che ancora esula dall'esperienza quotidiana di ciascuno, è infatti importante anzitutto delineare con chiarezza i tratti del fenomeno della cui possibile regolazione penalistica si va indagando. Così, si analizzeranno i differenti "livelli" di automazione che le *self-driving cars* possono presentare, distinguendo in particolare tra mezzi semi-autonomi e veicoli totalmente autonomi. Poi, si osserveranno le future prospettive evolutive di implementazione della tecnologia *self-driving*, muovendo dal concetto penalistico di rischio consentito, e dunque dal complesso e mutevole bilanciamento che vede contrapposti, ai benefici sociali promessi, i rischi, reali o supposti tali, connessi proprio all'innovazione tecnologica in questione.

Con la seconda sezione (§§ 4-5) si entrerà poi nel vivo della trattazione più schiettamente penalistica, affrontando il tema centrale dei *reati colposi di evento* (morte o lesioni) connessi al verificarsi di un incidente stradale. Potrà continuare a risponderne il conducente – e se sì, in che termini? Assumeranno profili significativi di responsabilità figure altre rispetto a quest'ultimo, quali il costruttore, o soprattutto il programmatore del mezzo? Cercheremo di rispondere a questi interrogativi proprio muovendo dalla distinzione, sopra accennata, tra veicoli semi-autonomi e vetture completamente *self-driving*.

Una terza parte (§ 6) sarà dedicata ad approfondire gli effetti dell'introduzione dell'*autonomous driving* rispetto alla *tutela anticipata della sicurezza stradale* in chiave penalistica, ovvero circa quei reati che generano o incrementano il *pericolo* del verificarsi di sinistri. Così, si guarderà ai reati stradali in senso stretto attualmente esistenti, ovvero a quegli illeciti che proibiscono alcune condotte di guida (o alla guida) in ragione della loro intrinseca pericolosità: cercando di ipotizzare in che misura tali fattispecie saranno ancora integrabili, oppure necessiteranno di modifiche, a seguito della diffusione della guida autonoma.

Una quarta sezione (§ 7), infine, getterà brevemente lo sguardo sull'eventuale esigenza di introdurre nuove fattispecie atte a fronteggiare l'inedita pericolosità introdotta dalle tecnologie *driverless*, facendo particolare riferimento – per tutti – al complesso e articolato nodo della *cybersecurity*.

2. Dalle auto semi-autonome a quelle totalmente *self-driving*: i "livelli" di automazione.

Il necessario punto di partenza, per i motivi già detti, è dunque rappresentato dall'approfondimento di alcuni aspetti di carattere generale dell'*autonomous driving*. Anzitutto: in che cosa consiste esattamente tale tecnologia?

In termini molto generali, potremmo dire che essa coinvolge un ventaglio estremamente variegato di gradi e modi di partecipazione dell'intelligenza artificiale alla conduzione del mezzo. In primo luogo, l'automazione veicolare può coinvolgere solo alcune, o più, funzioni di guida. Alcuni tipi di automazione, ad esempio, riguardano solo le funzioni di accelerazione e freno, ma non anche quella dello sterzo, o il contrario. Ancora, entro ogni singola funzione di guida il computer può assumere un ruolo più o meno significativo rispetto all'apporto del "passeggero-conducente potenziale" umano.

All'intuibile complessità dello scenario tecnico, soccorre la presenza di numerosi standard – elaborati da enti di categoria a carattere nazionale o internazionale – articolati su una scala di "livelli" di automazione "complessiva" del mezzo, da utilizzare come "metro" di riferimento per classificare le singole vetture.

Per tutti, possiamo qui riferirci al più diffuso standard J3016 della *SAE International* (*Society of Automotive Engineers*), stilato nel 2014 e rivisto, da ultimo, nel 2018, il quale si articola

(2017), Hilgendorf (2017), in particolare pp. 181 ss. Per uno sguardo alla situazione giapponese, cfr. Matsuo (2017), in particolare pp. 163 ss. Più in generale, la quantità di scritti (essenzialmente negli USA) dedicati alle *autonomous cars*, nei loro aspetti giuridici più generali, è a dir poco alluvionale: nelle note che seguono si è cercato di selezionare, fra tutti, i lavori più significativi. Tra i lavori più generali sull'*autonomous driving*, si indicano invece fin d'ora, per tutti, alcuni ampi volumi collettanei: oltre alla serie in (finora) cinque volumi, Meyer e Beiker (eds.), rispettivamente (2014), (2015), (2016), (2018) e (2019), si veda Mauer *et al.* (eds.) (2016).

su sei livelli, oscillanti da 0 a 5[9]. Sebbene esistano altri importanti standard, pur tutti tra loro abbastanza similari[10], a fini semplificatori ci limiteremo – qui e nel prosieguo del lavoro – a utilizzare soltanto quest'ultimo.

Il livello 0 (*No Driving Automation*) riguarda i veicoli privi di qualunque tipo di automazione. I livelli 1 (*Driver Assistance*) e 2 (*Partial Driving Automation*) si riferiscono invece a mezzi in cui è ancora attivamente presente un guidatore umano, mentre la macchina è in grado di controllare la frenata/accelerazione e lo sterzo, alternativamente al livello 1 e cumulativamente al livello 2. Tali livelli non corrispondono ancora, tuttavia, alle *self-driving cars* vere e proprie. Piuttosto, si tratta di sistemi di automazione già presenti in alcuni modelli di auto in commercio – in special modo il livello 1 – e il cui utilizzo può comunque considerarsi già autorizzato da parte dell'ordinamento italiano: in ragione, per l'appunto, della necessaria presenza costante e attiva del guidatore umano, non sostituito ma soltanto "aiutato" o "facilitato" dal mezzo medesimo.

A partire dal livello 3 (*Conditional Driving Automation*) si entra invece nel mondo delle *self-driving cars* vere e proprie. A tale livello, più in particolare, la macchina è già capace di condursi da sola in condizioni ordinarie, pur conservando i comandi di guida e la figura del guidatore. Quest'ultimo è chiamato non tanto a operare attivamente in modo continuativo, quanto piuttosto a intervenire nel caso in cui la macchina segnali la necessità di prendere il controllo manuale del mezzo, o in altri casi di emergenza. Potremmo dunque parlare, con riferimento a tali tipi di auto, di vetture *semi-autonome*.

I livelli 4 (*High Driving Automation*) e 5 (*Full Driving Automation*), infine, si riferiscono a mezzi tecnicamente capaci di guidarsi da soli senza necessità di controllo umano costante. Al livello 4, l'auto già consente al conducente di dedicarsi ad altre attività durante gli spostamenti, potendo il mezzo affrontare autonomamente la grande maggioranza degli scenari possibili, compreso il viaggio senza passeggeri: nel caso in cui si presentino circostanze non governabili dal sistema, la vettura è programmata per arrestarsi. Quest'ultima conserva ancora, tuttavia, i comandi manuali, per permettere a un eventuale passeggero capace di guidare di prendere in mano il volante e gestire eventuali circostanze eccezionali, non governabili dal mezzo.

Il volante e i pedali, invece, scompaiono del tutto nelle vetture con automazione di livello 5, potendo esse affrontare da sole qualunque scenario di guida che sarebbe gestibile da un operatore umano. Assieme ai comandi, evidentemente, scompare la figura del conducente che, sia pure in via solo potenziale, permaneva anche a livello di automazione 4. Tutti gli occupanti del veicolo – se ve ne siano – sono dunque egualmente passeggeri: è il caso, ad esempio, dei futuribili *robotaxi*. Pertanto, si può certamente dire che i mezzi di livello 5 siano i soli davvero *completamente autonomi*[11].

Quelli di livello 4, invece, rimanendo "a metà del guado", rientrano nella categoria che pone le maggiori difficoltà di regolazione giuridica. Tra i due modelli sopra proposti, in ogni caso, si tenderà probabilmente – lo vedremo meglio più avanti – a schiacciare la loro disciplina sul modello della semi-autonomia[12].

3. Le prospettive evolutive della disciplina giuridica della guida autonoma, tra bilanciamento e rischio consentito.

La scansione appena descritta in livelli, invero, sembra corrispondere, a grandi linee, alle prospettive future di sviluppo dell'*autonomous driving* e della sua introduzione all'interno della società. Come accennato, i primi – fino forse al secondo – corrispondono a un grado di autonomia del veicolo che, pur essendo riconducibile più a una "assistenza computerizzata" del mezzo, piuttosto che a una vera e propria guida senza un conducente umano attivo, è già oggi

[9] SAE International (2018).

[10] Ad esempio, per tutti, lo standard dapprima proposto negli USA dell'agenzia *National Highway Traffic Safety Administration* – NHTSA (2013) – articolato su 5 livelli. Sul modello LoRicco (2018), pp. 301-303. Per un confronto tra le varie scale v. Glancy (2015), pp. 630 ss.

[11] Sulla distinzione tra mezzi semi-autonomi e completamente autonomi, per tutti, Surden e Williams (2016), pp. 131 ss.

[12] V. *infra* il § 4.

una realtà commerciale. Ma pare verosimile che con riferimento alle *self-driving cars* vere e proprie – quelle con automazione di livello 3, 4 o 5 – non si assisterà all'introduzione di un regime autorizzatorio di punto in bianco, quanto piuttosto a una disciplina giuridica graduale e progressiva[13].

Quasi certamente, infatti, le auto tradizionali verranno dapprima affiancate da vetture semi-autonome con la presenza obbligatoria del conducente; per poi transitare solo più tardi verso scenari caratterizzati da una più intensa automazione dei mezzi di locomozione, fino alla vera e propria scomparsa del guidatore.

La gradualità di tale evoluzione chiamerà le progressive fasi tecnologiche, che via via verranno autorizzate, a confrontarsi con problematiche differenziate di regolazione giuridica, e dunque anche penalistiche. In particolare, proprio quanto ai riflessi sul diritto penale, sarà di fondamentale importanza – come vedremo meglio più avanti – la distinzione poc'anzi delineata tra vetture semi-autonome e quelle che lo siano totalmente.

Per comprendere e prevedere gli scenari futuri di apertura dei vari ordinamenti all'*autonomous driving* è possibile avvalersi del concetto penalistico di rischio consentito[14]. Come noto, tale nozione si fonda su una logica di bilanciamento tra due poli contrapposti. Per stabilire l'entità del "rischio tollerato", entro un certo quadro di sviluppo tecnologico e di sensibilità sociale, si dovranno infatti – da un lato – considerare i benefici collettivi derivanti da una certa attività. Dall'altro, invece, sarà imprescindibile tenere conto dei rischi ad essa connessi, valutati sia sotto un profilo di entità scientifico-oggettiva, sia di percezione dal punto di vista "soggettivo" della società[15].

La gradualità della progressiva e sempre più ampia autorizzazione e diffusione dell'*autonomous driving* sarà l'effetto ineludibile dell'evoluzione nel tempo di tale complessa dialettica. La concretizzazione dei benefici sociali da tale tecnologia promessi, infatti, andrà pian piano a costituire un contraltare sempre più attraente e capace di esorcizzare quei rischi prospettati da atteggiamenti, al contrario, ispirati a logiche di precauzione. Oltretutto, è ragionevole supporre, sia pur parlando in termini generalissimi, che il passare del tempo gradualmente addolcirà le stesse ritrosie sociali e i timori legati alla nuova tecnologia. Via via che i consociati inizieranno a familiarizzare con la guida autonoma, l'"ignoto tecnologico" a essa correlato diventerà sempre meno ignoto. Ciò, evidentemente, permetterà prospettive autorizzatorie sempre più ampie.

3.1. *I benefici sociali.*

La tecnologia della guida autonoma pare essere particolarmente generosa quanto a *benefici sociali*. Tali vantaggi, peraltro, sono destinati a crescere sempre di più, sia di numero che di intensità, via via che il livello di automazione dei veicoli autorizzato dall'ordinamento sarà sempre più elevato, oltre che in base all'incremento del grado della loro concreta diffusione sulle strade[16].

Il beneficio principale da considerare è senza dubbio quello della *sicurezza stradale*. Vari studi hanno mostrato come la diffusione dell'*autonomous driving* condurrebbe a una drastica riduzione del numero di incidenti e delle relative vittime[17]. Ben il 90% circa dei sinistri, infatti, deriverebbe da cause umane[18]: conseguenza di consapevoli violazioni del Codice della strada, provocati dallo stato di intossicazione da alcool o stupefacenti del conducente, oppure – più semplicemente – risultato di umana disattenzione.

[13] Sebbene le sperimentazioni attuali già abbraccino vetture di vari livelli, con progetti di auto semi-autonome (ad esempio, *Tesla* modello S) che si affiancano a più ambiziosi programmi di sviluppo direttamente di auto completamente automatiche (è l'esempio delle *ex Google cars*, adesso *Waymo*). Sulla differenza tra i due approcci, in una prospettiva futura, cfr. Pearl (2017), pp. 29 ss.

[14] Su di esso, per tutti, Militello (1988), in particolare pp. 55 ss. (il quale tuttavia predilige la dizione "rischio adeguato") nonché Forti (1990), pp. 250 ss.

[15] Sul bilanciamento rischi-benefici in termini etici v. Hevelke e Nida-Rümelin (2015), pp. 621 ss. Per uno scenario complessivo, cfr. Milder (2018).

[16] Per tutti, Hilgendorf (2017), p. 174.

[17] Fra tanti: Hanlon (2016), p. 3, Pearl (2017), pp. 35 ss., Beiker (2012), pp. 1149-1150, LoRicco (2018), pp. 303-304.

[18] Feldle (2017), p. 195, Coca-Vila (2018), p. 60.

Le *self-driving cars*, invece, non sarebbero evidentemente esposte ai rischi di "distrazione" o "intossicazione" né – è da immaginarsi – violerebbero mai in modo deliberato le regole di circolazione, essendo programmate per rispettare scrupolosamente il Codice della strada[19] (salvo forse i casi di emergenza). Ancora, grazie ai propri sensori, "vedrebbero" le altre macchine in situazioni nelle quali, invece, un conducente umano non avrebbe potuto rendersi conto della loro presenza, riducendo così ulteriormente il rischio di incidenti.

Finché le *autonomous cars* circoleranno a fianco dei veicoli tradizionali, rimarranno sempre dei fattori di rischio connessi a tale commistione, e in particolare all'imprevedibilità del comportamento umano al volante da parte degli schemi algoritmici perfettamente razionali propri dei mezzi computerizzati; oppure, viceversa, all'enigmaticità della condotta robotica rispetto ai canoni comportamentali tipici dell'uomo. Anzi, in tale prima fase proprio la "comunicazione" tra veicoli autonomi e utenti umani della strada – pedoni e auto tradizionali – rappresenterà probabilmente uno dei principali problemi della circolazione stradale[20].

In una fase di automazione del traffico più avanzata, in cui la totalità o quasi dei mezzi saranno vetture autonome[21], si suppone che invece prevarrà un più efficiente atteggiamento del tutto cooperativo, potendo peraltro i vari utenti "artificiali" della strada interagire e scambiarsi informazioni via *cloud computing*[22]. Ma, certo, anche allora l'abbattimento dei sinistri non potrà mai essere totale[23]. Torneremo tuttavia su questo punto più avanti[24].

Ulteriori benefici derivanti dalla diffusione della guida autonoma risiedono nell'incremento dell'*efficienza della circolazione* veicolare, resa più rapida e fluida da capacità sensoriali e tempi di reazione sconosciuti ai guidatori umani, nonché dall'atteggiamento cooperativo dei mezzi tra di loro, in luogo della conflittualità che ogni utente della strada ben conosce[25]. Ciò permetterebbe un notevole *risparmio di tempo* per gli spostamenti, oltre che un *risparmio di carburante* a tutto beneficio dell'*ambiente*[26]. Ancora, benefici sarebbero poi gli effetti sulla *salute* legati alla riduzione dello stress traffico-correlato, massimi nel caso delle vetture totalmente autonome, che permetterebbero agli utenti di dedicarsi ad attività diverse rispetto alla guida. Certamente, poi, si avvantaggerebbe anche la *produttività* complessiva e dei singoli, mediante la riduzione dei "tempi morti" oggi spesi al volante[27].

[19] *Contra* Schimelman (2016), pp. 348 ss. In tal senso, invece, Gurney (2015), p. 413. Lo stesso si interroga se le violazioni del Codice della strada – siamo in ambito statunitense e si tratta perlopiù di illeciti penali imputabili oggettivamente (*strict liability*) – dovrebbero comunque essere addossate al conducente in base al mero nesso causale. La risposta è negativa, salvo comunque pragmaticamente auspicare un mutamento solo graduale delle regole vigenti (pp. 414 ss.). Scettico, invece, Westbrook C. (2017), p. 106. Sul punto v. anche Glancy (2015), pp. 661 ss.

[20] Per tutti, Surden e Williams (2016), pp. 150 ss.

[21] Forse, addirittura, si arriverà un giorno alla proibizione della guida umana su strada. A un certo livello di sviluppo tecnologico, svaniti i timori relativi ai rischi correlati a una tecnologia ancora da rendere familiare ai consociati, la pericolosità statistica della guida tradizionale rispetto all'*autonomous driving* non potrà (forse) più ritenersi controbilanciata dalla mera "utilità sociale" del "piacere di guidare manualmente", che andrebbe così confinato in eventi o situazioni circoscritte (come le gare automobilistiche).

[22] Hilgendorf (2017), p. 173. Sui tipi di connettività tra veicoli autonomi Glancy (2015), pp. 640 ss.

[23] Marchant e Lindor (2012), p. 1321, Coca-Vila (2018), p. 60, Hevelke e Nida-Rümelin (2015), p. 620.

[24] Cfr. *infra* § 5, per quanto attiene le conseguenze a livello di imputazione penalistica di eventi lesivi cagionati da veicoli completamente autonomi.

[25] Pearl (2017), pp. 39-40, Beiker (2012), pp. 1150-1151, e *amplius* Mauer *et al.* (eds.) (2016), pp. 301 ss. Sui benefici *lato sensu* economici dell'*autonomous driving* Thierer e Hagemann (2015), pp. 351 ss.

[26] Hanlon (2016), pp. 4-6, LoRicco (2018), p. 305. V. però Butti (2016), pp. 447-451, che parla di "ambivalenza ambientale" dell'*autonomous driving*, individuando in esso anche alcuni possibili profili di rischio per l'ambiente.

[27] Hanlon (2016), p. 6, Pearl (2017), pp. 40-4, LoRicco (2018), p. 305. Le vetture completamente autonome, peraltro, sarebbero dotate della capacità di parcheggiarsi da sole: il che comporterebbe non soltanto un ulteriore risparmio di tempo, ma prelude anche a mutamenti particolarmente incisivi non solo sulle modalità di progettazione degli edifici di nuova costruzione (rivincita della *lobby* sul *garage*), ma anche più radicalmente sull'urbanizzazione e la conformazione delle stesse città del futuro (Zakharenko (2016)). Si potranno – solo per fare alcuni esempi – allocare le aree di parcheggio lontano dagli edifici e dai centri cittadini, eliminare negli stalli di sosta gli ormai "inutili" spazi per l'apertura delle portiere, o addirittura ripensare le stesse barriere attualmente esistenti tra i concetti di vettura privata, *car sharing*, *taxi* e mezzo pubblico, mediante il ricorso a veicoli autonomi che girino per le strade delle città, allocati da algoritmi che riducano al massimo le improduttività, senza dover mai fermarsi o parcheggiare (Grush e Niles, (2019), pp. 87 ss.). Cfr. altresì, su tali temi, Levinson (2015) pp. 798 ss.

Infine, ma non meno importante, è il fatto che il raggiungimento di una completa automazione veicolare permetterebbe di *mobilizzare categorie di persone finora impossibilitate a muoversi autonomamente*: anziani con difficoltà, disabili, minori, o semplicemente persone prive di patente[28]. O addirittura soggetti sotto l'effetto di alcool o droghe, "sterilizzando" così la loro pericolosità alla guida[29].

3.2. *I profili di rischio, tra percezione sociale e logiche di precauzione.*

La prospettiva allettante dei benefici sociali derivanti dall'*autonomous driving*, però, deve fare i conti anche con la dimensione dei *rischi*, veri o presunti tali, che da tale tecnologia discenderebbero[30].

Dal punto di vista della *pericolosità oggettiva*, abbiamo già ricordato come la sicurezza stradale paia destinata a giovarsi enormemente della tecnologia della guida autonoma. Se il numero complessivo dei sinistri è destinato a scendere drasticamente, in ragione dell'eliminazione della gran parte di collisioni di derivazione umana, è pur vero che residuerebbe quel piccolo gruppo di eventi lesivi i quali si sarebbero comunque verificati – a prescindere dal tipo di guida, autonoma o manuale – in quanto aventi perlopiù derivazione "esterna" rispetto ai comportamenti degli attori della circolazione stradale. Inoltre, in uno scenario di *autonomous driving*, a tale ineliminabile "zoccolo duro" di rischio, presente in ogni caso, andrebbe aggiunta una quota, *pur statisticamente piccola ma inevitabile*, di danni derivanti proprio dalla guida autonoma medesima, a essa connaturati. Malfunzionamenti dell'intelligenza artificiale alla guida, infatti, pur statisticamente rari, sono inevitabili. Possono essere previsti, in parte, a livello appunto statistico-generale: ma mai, certamente, a livello concreto, in relazione ai singoli casi.

Peraltro, a dimostrazione di quanto appena detto, rischi connessi alla tecnologia *self-driving* si sono *già* concretizzati nella sperimentazione pratica. I primi sinistri verificatisi, di minore entità, non hanno avuto una grande eco mediatica, sebbene sia possibile tenerne traccia grazie a fonti ufficiali[31]. Ma le notizie dei primi incidenti mortali – quattro dal 2016 alla fine del 2018 – sono rimbalzate ai quattro angoli del globo[32].

Ai profili oggettivi di rischio connessi ai possibili malfunzionamenti del veicolo autonomo, nebulosi nei loro contorni ma quantomeno grossomodo inquadrabili, ne vanno peraltro aggiunti di ulteriori, ancora più insidiosi, cioè quelli imprevedibili anche nei loro termini più generali finché non si arrivi davvero a un loro concreto manifestarsi. L'esempio più emblematico di tali inediti e sfuggenti profili di rischio, per tutti, è la recente questione della *cybersecurity* e del rischio *hacking* in relazione alle *self-driving cars*, su cui pure torneremo[33].

[28] Beiker (2012), pp. 1151-1152, Pearl (2017), pp. 41-43, LoRicco (2018), p. 307. Più diffusamente, sui rapporti tra *autonomous driving* e disabilità, v. *amplius* Francis (2018) e Westbrook H. (2018).

[29] Sul *drunk driving* v. *infra* l'ultima parte del § 6.

[30] Per un panorama generale cfr. Taeihagh e Si Min Lim (2019), pp. 106 ss.

[31] Nello Stato della California, ad esempio, il sito ufficiale del *Department of Motor Vehicles* riporta tutti i sinistri che hanno coinvolto *autonomous cars*. La legislazione californiana, infatti, ne obbliga la segnalazione alle pubbliche autorità, con apposito modulo, fin dal primo momento in cui è stata autorizzata la circolazione in via sperimentale di tali veicoli, a fini proprio di monitoraggio pratico dei rischi e trasparenza nei confronti della pubblica opinione. Al 12 febbraio 2019 erano state ricevute un totale di 133 segnalazioni: State of California Department of Motor Vehicles (2019).

[32] Il primo incidente ad aver provocato la morte del conducente, in ordine temporale, avveniva – in realtà senza troppa risonanza – a Handan (Cina) il 20 gennaio 2016. Il primo vero caso mediatico si è avuto pochi mesi più tardi a Williston (Florida, USA), il 7 maggio 2016, quando una vettura *Tesla* modello S si infilava sotto ad un camion bianco, non riuscendo a distinguerlo dal cielo luminoso, distruggendo completamente l'abitacolo e provocando così la morte del conducente (cfr. Hanlon (2016), pp. 11-13, Tronsor (2018), pp. 217-218, Pearl (2017), pp. 20 ss.). Ancora più forte era la risonanza sui media del terzo incidente, probabilmente perché per la prima volta a morire non era il conducente – magari pilota collaudatore professionista – ma un pedone qualunque. Il sinistro avveniva a Tempe (Arizona, USA) il 18 marzo 2018, e per la prima volta coinvolgeva una vettura completamente autonoma, di *Uber* (LoRicco (2018), pp. 308-309). Un quarto incidente fatale, infine, con morte del conducente, accadeva pochi giorni dopo, il 23 marzo 2018, a Mountain View (California, USA).

[33] Cfr. *infra* § 7. Peraltro, v'è da dire come tali fattori di pericolo, per quanto a livello oggettivo-scientifico si presentino come i più inquietanti, proprio in ragione dell'impossibilità di prevederne financo l'ordine di grandezza, sono i

Riassumendo, potremmo dire che già l'entità oggettiva dei rischi dell'*autonomous driving* appare sfumata. Con certezza, sappiamo solo che essa è meno incisiva dei pericoli connessi alla guida tradizionale. Ci sfugge, tuttavia, una sua esatta qualificazione e quantificazione[34]. Un tipo di risultato, questo, va detto peraltro, che è del tutto coerente con il progressivo dispiegarsi della *Risikogesellschaft* nella contemporaneità tecnologica.

Ma è sul *versante soggettivo* della *percezione sociale dei rischi* che si gioca evidentemente la partita più significativa: e qui, più di tutti, proprio la riflessione – sociologica e non solo – sulla "società del rischio" risulta particolarmente illuminante.

Il concetto di rischio che viene in rilievo non è infatti un *quantum* assoluto, dalla sola portata probabilistico-oggettiva: ma un rischio *tollerato*, *accettato* dalla società. Esso, dunque, scaturisce da un giudizio di tipo (complessivamente) politico-valutativo, che si fonda non solo su granitici dati scientifici, ma anche sui mutevoli umori sociali, dalla più varia origine, che ne condizionano la sua percezione e percepibilità[35]. Non si esagera, probabilmente, nell'affermare come la tollerabilità sociale di un rischio sovente affondi le sue radici più profonde non tanto nella sua dimensione oggettiva, scientifica, quanto piuttosto in deformanti pregiudizi e paure anche irrazionali, in larga parte legati fortemente al momento comunicativo del supposto pericolo.

La ricerca empirica ha avallato l'intuizione di molti circa la significativa portata di tali timori, privi di solido fondamento razionale, che il pubblico tende a nutrire rispetto alle tecnologie di guida autonoma, similmente a quanto accade con tanti altri prodotti della scienza. Non a caso, ad oggi la maggioranza degli intervistati afferma di fidarsi di più delle proprie capacità di guida rispetto a quelle di un mezzo a guida autonoma: pur contro ogni evidenza statistica oggettiva, che assegna a quest'ultimo un grado di sicurezza comunque sempre più elevato rispetto anche al più attento dei guidatori umani[36].

Il paradosso si fa ancora più manifesto nel programmare la macchina rispetto alla condotta da tenere quando, tragicamente, la situazione concreta permetta solo di scegliere tra scenari alternativi comunque nefasti per qualcuno[37]. È meglio che la vettura autonoma investa il bambino che si inserisca nella sua traiettoria all'improvviso uccidendolo, oppure che esca dalla carreggiata e si vada a schiantare contro un ostacolo, sacrificando così il suo passeggero? Queste affascinanti quanto complesse riedizioni del *Trolley problem*[38] non sono affatto dei meri esercizi di stile, dall'effetto pratico limitato a pochissimi casi che potremmo inquadrare

---

meno rilevanti a livello di percezione dell'opinione pubblica. Tale sottovalutazione dipende probabilmente dalla scarsa informazione circolante sul punto, peraltro non veicolata finora da eventi eclatanti di concretizzazione del pericolo, a differenza di quanto accaduto invece rispetto agli episodi mortali di incidenti provocati proprio da un malfunzionamento dell'IA (su cui v. *supra* la nota precedente).

[34] Cfr., ad esempio, l'indagine sperimentale di Teoh e Kidd (2017).

[35] In ambito sociologico, per tutti, oltre a Beck U. (1986), in particolare pp. 38 ss., cfr. anche Giddens (1990), pp. 125 ss., e Luhmann (1991), pp. 40 ss., 182 ss. Tra i penalisti, per tutti, Silva Sánchez (2011), pp. 26-27, Piergallini (2004), pp. 16 ss. e Mendoza Buergo (2001), pp. 24 ss. Più in generale, cfr. Donini (2004), pp. 107 ss. e, da ultimo, Palazzo e Viganò (2018), pp. 102 ss.

[36] LoRicco (2018), pp. 308-309, riporta gli interessanti risultati di varie ricerche. Secondo esse, tre americani su quattro si dicevano spaventati all'idea di viaggiare su una *self-driving car*, mentre solo uno su cinque affermava di fidarsi del fatto che una macchina si guidi da sé. La spiegazione data dall'84% dei contrari all'*autonomous driving* era che si fidavano più delle proprie capacità di guida che della tecnologia. Hilgendorf (2017), p. 175, correttamente dunque paventa il rischio che i veicoli autonomi vengano percepiti da molti come «*killjoys*». Cfr. anche gli studi statistici di Raue *et al.* (2019).

[37] Rispetto a tali casi vi è ormai una letteratura, se non ampia, comunque non trascurabile. Per tutti, v. l'ampio saggio (in inglese) di Coca-Vila (2018) – oppure in versione spagnola Coca-Vila (2017) – oltre a Wolkenstein (2018), Pugnetti e Schläpfer (2018), Tronsor (2018), pp. 227 ss., Feldle (2017), Gogoll e Müller (2017), Leben (2017), Santoni de Sio, (2017), Contissa *et al.* (2017a) – anche in versione italiana, Contissa *et al.* (2017b) – Bonnefon *et al.* (2016), Goodall (2016), Nyholm e Smids (2016).

[38] Così sono denominati, in ambito anglosassone, tali "classici" dilemmi morali, a partire dalla formulazione di Philippa Foot (1967). Al contrario, secondo Nyholm e Smids (2016), in particolare pp. 1287-1288, la riconduzione di tali casi al dilemma morale del *Trolley problem* è ingannevole, in quanto sussistono vari punti di distacco da tale modello. Tra quelli evidenziati, sicuramente significativo è il primo, che consiste nel notare la differenza di contesto in cui si svolge la decisione etica: quello concitato dell'azione da un lato, e quello algido e distaccato della programmazione *ex ante* dall'altro.

come stato di necessità del "conducente", ma assumono un ruolo centrale rispetto alla generale percezione della pericolosità dell'*autonomous driving* da parte degli utenti. Molti, moltissimi avrebbero paura a consegnare la propria incolumità nelle mani di un algoritmo, pronto a disporne secondo oscure e imprevedibili trame[39]: anche se ognuno di noi, nella vita di tutti i giorni, non si fa problemi ad affidarsi a ben più pericolosi conducenti umani[40].

La prospettiva di una standardizzazione legale di questi "algoritmi di necessità" – magari ancorandola, com'è stato proposto, al criterio etico consequenzialista del minimo danno[41] – inevitabilmente esporrebbe gli utenti al tanto paventato rischio di essere, in situazioni eccezionali, "sacrificati" dalla vettura. Ciò potrebbe portare a un "sabotaggio commerciale" di tali prodotti, con l'eventuale prospettiva di trascinare con sé gran parte dei benefici collettivi che dalla guida autonoma sarebbero potuti derivare[42]. Non meno problematica è tuttavia l'opposta prospettiva di veicoli autonomi a etica differenziata, magari regolabile da parte dell'utente – com'è stato provocatoriamente proposto – con un'apposita manopola[43].

Questa diffidenza nei confronti delle *self-driving cars*, e dell'ignoto tecnologico a esse connaturato, è così per adesso inevitabilmente destinata a tradursi, sul piano legislativo, in prese di posizioni prudenziali, ispirate da logiche di precauzione[44].

Ma non sarà sempre così. E comunque molto dipende anche dall'atteggiamento culturale complessivo dell'area di riferimento. Non è un mistero che la precocità delle sperimentazioni negli Stati uniti sia stata politicamente "consentita" da una sensibilità molto più "razionalista" – o forse "sconsiderata", a seconda del punto di vista – rispetto agli standard europei. E anche nel contesto americano, comunque, il verificarsi dei primi sinistri ha avuto un'eco pubblica non certo trascurabile: al punto da imporre politicamente battute d'arresto e rinvii nelle sperimentazioni[45].

Da questo lato dell'Atlantico, invece, per adesso prevale la prudenza, secondo una tradizione europea ormai consolidata di ossequio al principio di precauzione. Ma anche nel Vec-

[39] Cfr., in particolare, i risultati delle varie indagini statistiche riportate da Bonnefon *et al.* (2016). La maggior parte degli intervistati, in particolare, si sarebbe contraddittoriamente mostrata d'accordo circa il fatto che i veicoli autonomi "utilitaristici" sono i più "morali" in generale, pur continuando a preferire modelli "egoisti" per sé stessi (p. 1574). V. anche i test compiuti da Costantini e Montessoro (2016), pp. 100-102.

[40] Come rileva Butti (2016), p. 441, l'uomo tende molto di più a tollerare gli errori umani che quelli della scienza e della tecnologia.

[41] Per tutti, Gogoll e Müller (2017), in particolare pp. 694-696. Più articolata la posizione di Leben (2017), che propone l'utilizzo di un algoritmo che riproduca un approccio morale di tipo "rawlsiano". Invece Coca-Vila (2018), pp. 64 ss., sviluppa il suo contributo partendo dal rigetto di un puro e semplice consequenzialismo utilitarista. L'Autore, più in particolare, muove dall'assunto che, nel moderno diritto penale, anche le situazioni di necessità non sono (soltanto) radicate in principi "collettivistici" come quello del "male minore". Piuttosto, queste sono regolate da un ben più complesso bilanciamento tra il generale principio liberale del *neminem laedere* e l'operatività, nel caso concreto, di eccezioni fondate su logiche solidaristiche, riconducibili al criterio del "male minore". Tale bilanciamento prende in considerazione due parametri. Da un lato il grado di "colpa", rispetto alla causazione del fatto, dei soggetti coinvolti: il pericolante e la vittima stessa, su cui il primo voglia "scaricare" il pericolo gravante su di sé. Dall'altro, i beni giuridici coinvolti, o meglio il loro rango. Il "valore" delle offese in gioco, infatti, non è sempre "quantizzabile", in ragione della natura personale dei beni in questione. Due vite umane, insomma, non valgono di più di una singola vita (pp. 69-70). Sostanzialmente adesivi a tale posizione Feldle (2017), p. 200, e Hilgendorf (2017), pp. 189-190. Il principio di inviolabilità della dignità umana, che starebbe alla base di tale assunto, è stato ribadito dalla giurisprudenza costituzionale tedesca, relativa al noto caso in cui veniva dichiarata incostituzionale la normativa che permetteva l'abbattimento di aerei civili in caso di dirottamento terroristico – su cui, per tutti, v. Hörnle (2009). Sui fondamenti dello stato di necessità, per tutti, v. Viganò (2000) e Mezzetti (2000), in particolare pp. 153 ss.

[42] Contissa *et al.* (2017a), p. 367. Così pare emergere anche dall'indagine statistica di Bonnefon *et al.* (2016), p. 1575, mentre più cauti appaiono Pugnetti e Schläpfer (2018), pp. 11-12.

[43] Contissa *et al.* (2017a), pp. 369 ss. Contrario a personalizzazioni dell'etica del veicolo, Coca-Vila (2018), pp. 61, 63-64.

[44] Sul principio di precauzione in ambito penalistico, per tutti: Forti (2006), Giunta (2006), Ruga Riva (2006), Martini (2010), Castronuovo (2012) e Corn (2013). Parla significativamente ed efficacemente di «angoscia tecnologica» Stortoni (2004).

[45] L'investimento del pedone nel marzo 2018 a Tempa ha infatti imposto uno stop momentaneo alle sperimentazioni compiute da *Uber*, poi riprese alla fine dell'anno. Anche l'entrata in vigore delle modifiche alla legislazione californiana, autorizzanti la circolazione sperimentale di veicoli privi di conducente, ha subito un simile slittamento.

chio mondo qualcosa inizia a muoversi: la Germania, per prima, ha approvato una legge che autorizza alcune forme di guida autonoma[46]. L'Italia – lo abbiamo accennato poc'anzi – si è accodata, consentendo le prime sperimentazioni[47]. Altri Stati, probabilmente, col tempo seguiranno.

4. Reato colposo d'evento e vetture semi-autonome: il *control dilemma*.

Completato l'*excursus* a carattere generale sull'*autonomous driving*, indispensabile per armarci dello strumentario d'analisi necessario, è adesso possibile fare un passo avanti, approdando finalmente alle questioni a carattere penalistico in senso stretto.

Il primo nodo problematico nel quale ci imbattiamo è certamente quello del classico reato stradale colposo d'evento: chi risponderà delle morti e delle lesioni che seguano un sinistro provocato da un mezzo a guida autonoma?

Poiché peraltro, come detto in precedenza, la circolazione di tali veicoli è attualmente consentita dall'ordinamento italiano solo per le sperimentazioni munite di apposita autorizzazione ministeriale, la quale peraltro può essere concessa solo con riferimento a mezzi semiautonomi e con la presenza obbligatoria di un pilota umano a bordo in grado di riprendere i comandi, l'analisi non potrà che fondarsi su inquadramenti regolativi futuri almeno in parte *ipotetici*. Tenteremo quindi di coniugare la problematica rispetto a una pluralità di possibili scenari normativi di riferimento, concentrandoci in particolare su quelli che ci sembrano più realistici.

Per discutere dell'applicabilità del paradigma tradizionale del reato colposo d'evento agli eventi lesivi scaturenti dalla circolazione dei veicoli a guida autonoma il punto di partenza migliore – ci sembra – è quello, già più volte accennato, circa la partizione tra veicoli semi-autonomi e vetture *fully autonomous*. Fintantoché il mezzo è materialmente dotato di comandi manuali, infatti, si potrà sempre individuare un soggetto umano privilegiato cui imputare gli eventi cagionati: ovvero la tradizionale figura del *conducente*[48], sia pure rilevante qui soltanto a livello *potenziale*[49].

Come abbiamo già rilevato, nelle auto semi-autonome, a livello di automazione fino a 3, la stessa progettazione tecnica prevede la necessità che vi sia una persona che monitori costantemente il funzionamento del veicolo, pronta a intervenire in caso di emergenza. Per questa categoria di soggetti, appare difficile rompere la riconduzione delle loro responsabilità a quelle tipiche del conducente di un'auto tradizionale. Il conducente potenziale sarebbe dunque ancora investito di una *posizione di garanzia* rispetto agli altri utenti della strada, nonché rispetto ai propri passeggeri[50]. Più in particolare, l'*obbligo di controllo* – di quella fonte di pericolo che è

[46] Cfr. Losano (2017), al quale segue in appendice la proposta di legge discussa al *Bundestag* (pp. 10-25). Sul resto dei paesi europei cfr. il riassunto di Tranter (2016), p. 79, nonché da ultimo De Bruine e Werbrouck (2018), pp. 1150 ss.

[47] Cfr. *retro* il § 1.

[48] Ovviamente anche rispetto ai mezzi semi-autonomi, come già per i veicoli tradizionali, e come vedremo anche con riferimento alle vetture dotate di *full automation*, è possibile configurare una responsabilità di singoli soggetti umani all'interno dell'apparato industriale produttivo, secondo il paradigma del danno da prodotto. Tuttavia, come vedremo *infra* nel § 5, con riferimento alle auto completamente autonome paiono esservi degli "innovativi" profili di danno difficilmente riconducibili al produttore. Approfondisce, in ambito statunitense, già rispetto alle *semi-autonomous cars* il profilo del danno da prodotto Westbrook C. (2017), pp. 126 ss.

[49] Va infatti evidenziato come la nozione di "conducente" non sia attualmente definita dal Codice della strada. La questione se il "conducente potenziale" sia parificabile, in via interpretativa, al conducente di un'auto tradizionale – e quindi sottoposto ai relativi obblighi – ci pare debba avere una risposta inevitabilmente positiva, fintantoché permanga la possibilità materiale di riprendere il controllo manuale del mezzo in un qualunque momento. È proprio tale figura, infatti, che al pari del conducente più tradizionale *attiva una fonte di rischio* – il veicolo – altrimenti assente in natura. Per questo, il conducente potenziale rimane sempre responsabile del suo controllo, ovvero di dominare i profili di rischio che siano dominabili. Si veda *amplius* quanto sviluppato poco oltre.

[50] Hilgendorf (2017), p. 181-182. Così (pur in ambito statunitense) anche Douma e Palodichuk (2012), p. 1161. Similmente Westbrook C. (2017), pp. 138-139. *Contra*, invece, Gurney (2015), pp. 426 ss., ritenendo impossibile la prova della *mens rea* del conducente per i reati di *vehicular manslaughter*.

la *semi-autonomous car* stessa – verrebbe certamente rinvenuto nelle clausole generali iperelastiche di cui agli artt. 140 e 141 del Codice della strada[51]: che impongono al conducente – lo si ricorda – di «comportarsi in modo da non costituire pericolo […] per la circolazione», di «conservare il controllo del proprio veicolo» e di «essere in grado di compiere tutte le manovre necessarie in condizione di sicurezza, specialmente l'arresto tempestivo del veicolo entro i limiti del suo campo di visibilità e dinanzi a qualsiasi ostacolo prevedibile»[52].

Peraltro, le fattispecie applicabili, osserviamo qui incidentalmente, sarebbero comunque quelle di omicidio o lesioni *stradali ex* artt. 589 *bis* e 590 *bis* c.p., e non quelle colpose comuni di cui agli artt. 589 e 590 c.p. L'obbligo di controllo descritto, infatti, parrebbe comunque classificabile come norma «sulla disciplina della circolazione stradale»[53], al pari di tutte quelle regole di cautela la cui violazione dà luogo a responsabilità colposa per i conducenti di auto tradizionali.

Né, d'altronde, è ragionevolmente immaginabile uno scenario diverso, quantomeno per quei veicoli semi-autonomi il cui livello di automazione non sia superiore a 3. Ben difficilmente il legislatore potrebbe costruire un'area di non punibilità per i "conducenti potenziali" di tali mezzi, configurando standard di cautela inferiori rispetto a quelli suggeriti dalla stessa tecnica come opportuni.

Diverso è invece il discorso rispetto alle vetture con livello di automazione pari a 4. In esse, la creazione di uno spazio almeno parziale di non punibilità per il "conducente" – qui, come s'è visto, ancora "potenziale", ma soltanto in via assolutamente eccezionale – parrebbe porsi come un'opzione politica passibile di essere considerata dal legislatore. Con una scelta simile, a livello di regolazione giuridica tali vetture passerebbero a essere assimilabili a quelle davvero completamente autonome, ovvero quelle con livello di automazione 5. Va anche detto, tuttavia, che escludere la figura del conducente dal novero dei possibili soggetti responsabili non semplifica certo le cose, ma al contrario le complica ulteriormente, come vedremo più oltre, quando tratteremo delle vetture completamente autonome[54].

Tornando alla questione principale, ovvero le modalità con cui un certo evento lesivo provocato da un sinistro stradale sia imputabile al "conducente" della vettura semi-autonoma, il paradigma ascrittivo *commissivo* tradizionale pare divenire – almeno in certi casi – *omissivo*.

Nella colpa stradale ordinaria, infatti, è noto come l'elemento imprudente, anche qualora consista effettivamente in una mancanza di un qualcosa, non rilevi tanto come omissione in sé, quanto piuttosto come un'omissione inserita in una condotta più ampia – la guida del veicolo – avente carattere complessivo indiscutibilmente commissivo. In fondo, la dottrina ha da sempre evidenziato la presenza di un momento omissivo in ogni tipo di colpa: ogni violazione cautelare, anche attiva, può essere sempre vista, allo specchio, come l'omissione di una cautela doverosa, del comportamento alternativo lecito[55].

Fintanto che il livello di automazione della *autonomous car* è basso – inferiore, e forse addirittura anche pari a 2 – il paradigma commissivo tradizionale rimane ancora inalterato. Il conducente non sorveglia un'attività "altrui", ma partecipa attivamente e continuativamente alla stessa. La macchina fornisce assistenza alla guida, ma di guida vera e propria da parte del conducente ancora certamente si può parlare. In un simile quadro, un'imprudenza di quest'ultimo non potrà che inserirsi in un più ampio contesto di azione che, in un'ottica complessiva, è indubbiamente classificabile come commissivo.

Ma con il crescere dell'automazione – a partire quantomeno dal livello 3 – l'attività del "conducente" trasmuta pian piano in mera sorveglianza, priva della necessità di qualsivoglia intervento attivo per lunghi periodi. Si immagini l'esempio di un soggetto che imposti il pro-

[51] Capaci cioè di introiettare, sotto l'egida formale della colpa specifica, per violazione delle leggi, la logica potenzialmente onnicomprensiva della colpa generica, direttamente fondata su un giudizio di prevedibilità dell'evento. Sui rapporti tra colpa generica e specifica, per tutti, Grotto (2012), pp. 61 ss.

[52] Rispettivamente art. 140, comma 1, e art. 141, comma 2, Codice della strada. Sul tema *amplius*, per tutti, Veneziani (2003a), pp. 588 ss., e Veneziani (2003b), pp. 187 ss.

[53] Secondo il testo degli artt. 589 *bis* e 590 *bis* c.p., ai loro primi commi. Su tali fattispecie v., senza pretese di esaustività, Schirò (2018), Dovere (2017), Addante (2017), Mattheudakis (2017), Bianchi (2016), D'Auria (2016), Notaro (2016), nonché, in volume, Pavich e Sturlese (2018), pp. 362 ss., Pollastrelli e Acquaroli (2017) e Menghini (2016).

[54] V. *infra* § 5.

[55] Per tutti, v. Giunta (1993), pp. 90 ss. Sulla distinzione tra azione e omissione, per tutti, Veneziani (2003b), pp. 44 ss.

prio mezzo semi-autonomo per un viaggio di molte ore, lasciando che l'auto corra da sé mentre lui si riposi, dorma, oppure lavori, o ancora si svaghi con un libro o un film. Se dopo varie ore di mancata sorveglianza la vettura provocasse un incidente, sembrerebbe difficile parlare di colpa commissiva, invece che omissiva. Diverso è il caso in cui la dovuta sorveglianza sia prestata, ma il conducente non si avveda della necessità di un suo intervento, oppure erri maldestramente nel porlo in essere: in tal caso, probabilmente si potrà parlare ancora di commissione, e non di omissione.

In definitiva, dal modello di evento lesivo cagionato commissivamente per colpa dai conducenti di veicoli tradizionali, rispetto alle *semi-autonomous cars* si passerebbe a un modello imputativo alternativamente commissivo od omissivo. Il conducente potenziale non sarebbe più responsabile per aver direttamente violato una qualche più o meno specifica regola cautelare stradale, ma per essere venuto meno all'obbligo di sorvegliare costantemente che la guida autonoma del veicolo non incorra in errori o malfunzionamenti; oppure per averlo sì fatto, ma male.

Al fondo, va detto che anche così rischia di restare sostanzialmente inalterata quella *tendenziale onnicomprensività della responsabilità del conducente per i fatti lesivi occorsi* che attualmente continua a essere pervicacemente predicata dalla giurisprudenza[56]. Dalla "clausola generale" del dovere di prudenza del conducente, che oggi implica la responsabilità per colpa sostanzialmente per qualunque evento si verifichi, pare ineludibile che si passi a una parimenti generale clausola di sorveglianza *omnibus*, che rinviene – di nuovo – nel medesimo soggetto – il conducente – il capro espiatorio perfetto cui addossare la responsabilità di qualsivoglia danno venga a realizzazione.

Né, d'altronde, è ragionevole attendersi un atteggiamento più permissivo da parte di una giurisprudenza che attualmente pare ancora rigorosissima nella tutela del bene dell'incolumità degli utenti della strada, anche a scapito del forzare i principi costituzionali di garanzia, anzitutto quello di colpevolezza.

Il tema qui, evidentemente, è sostanzialmente quello della ritrosia giudiziale nel dare spazio al principio di affidamento nell'ambito della circolazione stradale[57]: per cui l'agente viene sovente ritenuto responsabile del fatto materialmente cagionato anche quando non era concretamente prevedibile l'altrui comportamento[58]. Ciò, in nome di un generico e astratto, quanto inesigibile, dovere di "prevedere tutto", che poi altro non è se non il precipitato di preoccupazioni di ordine politico-criminale giudiziale di tutela rafforzata e onnicomprensiva dei beni primari in gioco[59].

Se dunque molto spesso lo stesso atteggiamento di consapevole (e imprevedibile) autoesposizione della vittima al pericolo *non è* ritenuto sufficiente per liberare da responsabilità il conducente, è facilmente immaginabile quale potrebbe essere l'atteggiamento della giurisprudenza rispetto a casistiche – come quella che qui interessa – in cui la fonte del rischio che il potenziale conducente è chiamato a dominare sia riconducibile *non* alla vittima, che rimane

[56] Il riferimento teorico principale di tale tendenza è ancora il risalente insegnamento di Duni (1964). Secondo tale opinione, è sufficiente che un evento di sinistro sia anche solo *astrattamente* prevedibile per poterlo imputare al conducente: «l'obbligo di prevedere concerne tutto quello che non si vede e che può verificarsi da un momento all'altro: fatti naturali, fatti umani altrui, prudenti o imprudenti, fatti propri (come ad esempio, un malessere) ecc. Questa previsione costituisce l'elemento essenziale della prudenza» (p. 323).

[57] Sul principio di affidamento in ambito stradale cfr., per tutti, Mantovani M. (1997), pp. 185 ss., Di Giovine (2003), pp. 19 ss., Veneziani (2003a), pp. 662 ss. e Veneziani (2003b), pp. 77 ss.; più in generale, v. Mantovani F. (2009) e Forti (1990), pp. 281 ss.

[58] Per tutte, Cass. Pen., Sez. 4, 22/6/2017, n. 45795, Passero, e Cass. Pen., Sez. 4, 25/6/2014, n. 46818, Nuzzolese. Il panorama giurisprudenziale appare variegato nelle formule lessicali utilizzate, ma sostanzialmente ancora molto lontano dal raggiungimento di una reale concretizzazione del rimprovero colposo. Fanno eccezioni sporadiche e isolate prese di posizione, fra cui spicca Cass. Pen., Sez. 4, 4/12/2009, n. 46741, Minunno, insolitamente netta nell'invocare il pericolo che, in mancanza di un inquadramento in concreto dell'imprudenza, si rischi di trasformare l'utente della strada nel «colpevole per definizione» o addirittura in un «capro espiatorio» (p. 5). La dottrina è critica rispetto al prevalente atteggiamento rigoroso della giurisprudenza: oltre ai contributi monografici citati alla nota precedente – ai quali potremmo aggiungere, nella manualistica, Palazzo (2018), pp. 329-331 e Fiandaca e Musco (2014), pp. 584 ss. (in particolare p. 587) – v. da ultimo D'Auria (2017), Russo (2010) e – sia consentito – Cappellini (2017).

[59] Sul punto sia ancora consentito, *amplius*, Cappellini (2017), pp. 653 ss.

dunque terza estranea, ma al mezzo autonomo medesimo.

Si comprende, perciò, come in tale scenario una qualche limitazione legislativa della punibilità per i conducenti delle auto semi-autonome, anche solo le più prossime alla completa automazione, appaia a dir poco irrealistica a uno sguardo disincantato. Non va dimenticata la diffusa diffidenza, o addirittura il timore, rispetto alle tecnologie *self-driving*, di cui abbiamo già parlato in precedenza. Se questo è il panorama in cui si arriverà ad autorizzare le prime *autonomous cars*, anche a livello commerciale, appare dunque molto probabile che si opterà per mantenere a ogni costo la (s)confortante figura "parafulmine" del "conducente", capace di attirare su di sé le colpe per qualunque evento occorso, indipendentemente dalla sussistenza di un reale e ragionevolmente esigibile potere di controllo degli eventi[60].

Non è un caso che questo problema sia stato definito in letteratura come *control dilemma*[61]: nonostante le potenzialità tecnologiche di autonomizzazione della guida, il conducente non verrebbe mai liberato da responsabilità, rischiando di rimanere, in definitiva, il capro espiatorio perfetto per qualunque eventualità lesiva si verifichi, anche imprevedibile e ingovernabile.

Questo risultato, tuttavia, oltre che in contrasto con il principio di colpevolezza, comporterebbe ulteriori effetti negativi sul piano pratico. Esso rischierebbe, anzitutto, di vanificare molti dei vantaggi promessi dall'*autonomous driving*. Si pensi a quella che potremmo chiamare la "liberazione dalla schiavitù del volante": la promessa della possibilità di dedicarsi ad altro mentre si è a bordo di una vettura *driverless* verrebbe vanificata dall'obbligo di sorvegliare costantemente l'operato della vettura[62]. Compito tanto mortificante quanto irrealizzabile efficacemente nella pratica. Studi scientifici hanno infatti chiaramente mostrato come l'attenzione e la velocità di reazione dell'uomo siano fortemente pregiudicate dal carattere passivo di un compito di mera sorveglianza, in luogo di uno attivo, quale la guida manuale[63]. Perdipiù, si arriverebbe al paradosso per il quale conducenti sempre più disabituati a guidare manualmente, in ragione dell'uso della tecnologia di guida autonoma, sarebbero chiamati a riprendere in mano il volante proprio nel momento più critico e difficile: ovvero nelle situazioni di emergenza[64].

Ma, in fondo, e più radicalmente ancora, è della stessa efficacia obiettiva in termini di riduzione della rischiosità, a livello globale, di cui è forse lecito dubitare. Se è difficile per il conducente potenziale umano accorgersi di quando vi è davvero una situazione di emergenza, è inevitabilmente molto alto il rischio di "falsi positivi": ovvero di situazioni in cui l'uomo, erroneamente convinto dell'esistenza di un rischio in realtà inesistente, intervenga manualmente in correzione della guida autonoma, ma provocando così, per davvero, un sinistro che altrimenti non si sarebbe mai verificato. Insomma, la possibilità stessa per il conducente di intervenire, soprattutto in scenari di elevata automazione, potrebbe addirittura finire per generare una quota di rischi superiore di quelli che l'operatività di un obbligo di sorveglianza è effettivamente in grado di prevenire[65].

[60] Tale meccanismo di "capro espiatorio" è analizzato a livello sociologico, per tutti, da Beck U. (1986), in particolare pp. 98-100. In ambito penalistico, Castronuovo (2009), pp. 86 ss., sviluppa l'attiguo tema di come la spiegazione istituzionale – e quindi prima di tutto giudiziaria – circa la causazione (colposa) di un fatto, svolga una funzione sociale lenitiva rispetto al comune sentimento di angoscia correlato alla paura dell'ignoto, e all'imprevedibilità e all'ineluttabilità del fato. Affermando la responsabilità di un singolo per aver cagionato quel danno, la società pare infatti psicologicamente rassicurata da tale simbolica riconduzione del fatto nell'ambito di ciò che è spiegabile, e quindi dominabile, prevedibile e potenzialmente prevenibile *pro futuro*, da parte del "sapere esperto" dell'uomo. Se è colpa di qualcuno, di un singolo, la tecnica – o meglio, la tecnologia – è innocente: e dunque riconfermata nella sua rassicurante infallibilità. Fiducia sociale, questa, ci pare importante sottolineare, tanto preziosa soprattutto in materie come quella che ci interessa, dove il sapere tecnico non ha solo la funzione di fronteggiare dei rischi preesistenti, ma altresì di contenere i pericoli da esso stesso generati.

[61] Hilgendorf (2017), pp. 181-182, 187-188.

[62] Beck S. (2016), p. 141.

[63] Schömig *et al.* (2015), Aria *et al.* (2016), Hevelke e Nida-Rümelin (2015), p. 624.

[64] Douma e Palodichuk (2012), p. 1164, che evocano lo spettro di una «intera generazione» nel futuro priva delle capacità di guida.

[65] Hevelke e Nida-Rümelin (2015), p. 624, Gurney (2015), p. 416.

5. L'addebito colposo del sinistro stradale nelle auto completamente autonome, fra danno da prodotto, imprevedibilità tecnologica e "vuoto" di responsabilità.

Ancora più complesso è il discorso che riguarda le *self-driving cars* ad automazione massima, cioè quelle completamente autonome.

Ad impossibilia nemo tenetur: la mancanza materiale dei comandi, evidentemente, fa venire meno la figura del potenziale conducente. Questi – divenuto mero passeggero del mezzo – potrà al più rispondere colposamente per mancanze nella manutenzione, che abbiano provocato il sinistro. Ciò, ovviamente, è possibile solo nel caso in cui si parli di un passeggero che sia anche proprietario della vettura, o comunque in una posizione tale per cui su di lui gravi un qualche obbligo giuridico di assicurare la piena funzionalità del veicolo.

Tutti i sinistri dovuti non a insufficiente manutenzione del mezzo, ma a un errore o un malfunzionamento del sistema di guida artificiale – per quanto numericamente esigui, come avevamo in precedenza accennato[66] –, non potrebbero così essere imputati a un "conducente", figura che qui neanche più esisterebbe. Chi ne risponderà, dunque?

Ove non si voglia esplorare la strada futuristica – per non dire fantascientifica – della responsabilità *diretta* del veicolo quale autonomo soggetto intelligente, prospettiva che ci pare – come minimo – ad oggi assolutamente prematura (se non forse proprio impossibile *tout court*)[67], non resta che cercare altre figure umane che possano rispondere, per colpa, degli eventi lesivi occorsi.

Il riferimento, qui, è alla possibile responsabilità dei *programmatori*, *progettisti* e *costruttori* del mezzo: in altri termini, dei vari soggetti inquadrati nel complesso apparato industriale produttivo delle autovetture autonome. All'infuori di questa colpa del *produttore*, non pare problematicamente residuare alternativa che ricondurre il fatto all'irrilevanza penale.

C'è un primo ordine di casi in cui sono individuabili soggetti umani potenzialmente responsabili nella catena produttiva. Tali ipotesi possono certamente essere inquadrate nella categoria penalistica della responsabilità per danno da prodotto, ormai indagata in letteratura, pur nella sua elevatissima problematicità[68].

V'è da dire, tuttavia, come il "prodotto" industriale in oggetto sia indiscutibilmente più complesso rispetto alle tipologie che solitamente vengono prese in considerazione[69]. E ciò non tanto con riferimento a eventuali errori che possono essere compiuti nella fase di progettazione e assemblaggio del mezzo, la quale tutto sommato non si distacca in maniera così netta rispetto a quanto già oggi avviene con riferimento alle auto tradizionali.

Piuttosto, l'inedita complessità sembra risiedere perlopiù nella fase di *programmazione* dell'intelligenza artificiale chiamata a governare il mezzo. La quantità di scenari che i programmatori sono chiamati a valutare è vastissima, e potenzialmente indefinita. Tutto ciò comporta l'intrecciarsi del lavoro di decine, se non centinaia di informatici, in un prodotto finale rispetto al quale è molto spesso arduo individuare *se* e *dove* ci sia stato davvero l'errore di un singolo programmatore[70]. È dunque difficile verificare se effettivamente vi sia un soggetto

[66] V. *retro* § 3.2.

[67] Sul tema della responsabilità diretta del soggetto artificiale vi è ormai una vasta letteratura, di cui possiamo qui dare soltanto riferimenti essenziali. Unico Autore a sostegno della sua configurabilità, già *de jure condito* (ma ragiona in termini di *common law*) è l'israeliano Gabriel Hallevy, di cui possiamo ricordare, oltre all'articolo dedicato espressamente al tema dei veicoli a guida autonoma Hallevy (2011/2012), anche i più generali lavori Hallevy (2015), Hallevy (2013) e Hallevy (2010). Il resto della dottrina, invece, nega ancora recisamente tale ipotesi. Per tutti, sul tema, cfr. Pagallo (2010), Pagallo (2011), Asaro (2012), Pagallo (2013), Freitas *et al.* (2014), Beck S. (2016), p. 141-142, Gless *et al.* (2016), pp. 415 ss., Riondato (2017), Lima (2018), Magro (2019), pp. 1201 ss., nonché, se consentito, il nostro Cappellini (2019a), cui si rinvia per più ampi riferimenti bibliografici.

[68] Il riferimento principale va all'ampia monografia di Piergallini (2004), ma si vedano già i suoi precedenti scritti Piergallini (1996) e Piergallini (1997), oltre al più recente, efficacissimo sunto della questione in Piergallini (2007). Sul tema v. altresì Castronuovo (2005).

[69] Cfr. Gless *et al.* (2016), pp. 426 ss.

[70] Beck S. (2017), p. 243. Merita richiamare il monito di Civello (2013), in particolare pp. 197 ss., che punta il dito contro il consolidarsi nella prassi – in situazioni di incertezza epistemologica come quella che qui interessa – di una figura denominata "colpa eventuale". In essa, il rimprovero colposo subirebbe una trasformazione genetica, ottenuta

che non abbia previsto qualcosa che ragionevolmente avrebbe dovuto prevedere, o che abbia mal implementato nel sistema la modalità di reazione del mezzo al presentarsi, nel traffico, di specifici dati concreti.

Tuttavia, si potrebbe ancora dire che, nei casi in cui l'errore tecnico di programmazione possa essere rilevato *con certezza*, i criticabili meccanismi individuati dalla giurisprudenza per imputare il danno da prodotto possono "ordinariamente" operare, sostanzialmente bypassando il problema della responsabilità del singolo programmatore e addebitando il fatto ai vertici aziendali. Ciò, evidentemente, potrà avvenire nel caso in cui i medesimi, dopo essere venuti a conoscenza del problema, non abbiano immediatamente provveduto a porvi rimedio: imponendo un aggiornamento obbligatorio del sistema di guida autonoma che sani la criticità rilevate, oppure – come *extrema ratio* – ritirando il prodotto dal mercato[71].

Ma il nodo davvero problematico, piuttosto, si presenta nei casi in cui il sinistro *non* si sia verificato a causa di un errore certo e riconoscibile nella programmazione: casi, dunque, tali da non "reggere" l'addebito dell'evento lesivo, financo in base a quei canoni giurisprudenziali che giudicano sufficienti dei profili di tipicità oggettiva e soggettiva "affievoliti" per imputare il danno da prodotto. Questo secondo ordine di ipotesi, invero, ha un evidente rilievo pratico, ponendosi – forse – in prospettiva addirittura come statisticamente più significativo del primo.

Anzitutto, va notato come le *self-driving cars*, al pari di tutti i robot guidati da intelligenze artificiali vere e proprie, non siano dei "classici", passivi prodotti-oggetto, ma in qualche modo almeno parzialmente *soggetti*, proattivi, dotati di *autonomia d'azione*. Ciò solo, già, rende più complesso ricostruire la trama causale dei loro comportamenti, nonché la misura della diligenza richiesta al produttore.

Ma c'è di più. Va infatti considerato come le intelligenze artificiali che comandano una vettura autonoma non funzionano soltanto in base a degli algoritmi integralmente preprogrammati, preimpostati dall'uomo – in altri termini, in base a degli schemi di comando *fissi*. Troppi sarebbero, infatti, gli scenari e le variabili da prendere in considerazione, per poter istruire la macchina sul comportamento "corretto" da adottare di fronte a ogni possibile situazione della strada e del traffico.

Così, per lo sviluppo delle tecnologie di *autonomous driving* – come per ogni altra applicazione dell'intelligenza artificiale allo stadio attuale dello sviluppo tecnico delle scienze robotiche – è inevitabile il ricorso al *machine learning*[72]. Grazie a esso, la macchina è in grado di apprendere dall'esperienza, divenendo così capace di affrontare un numero potenzialmente indefinito di scenari e variabili, pur a fronte di una quantità non illimitata di istruzioni che le siano state originariamente impartite.

Il risvolto negativo di tale tecnologia, tuttavia, risiede nel fatto che essa consente alla macchina di modificare i propri comportamenti, rispondendo agli *inputs* con reazioni a priori inevitabilmente *imprevedibili*[73]. Sovente neanche è possibile comprendere perché ha agito in un certo modo: gli algoritmi complessi attraverso cui opera, infatti, sono spesso definiti *black*

---

mediante una sostituzione surrettizia del giudizio di "prevedibilità" con quello di "non escludibilità" dell'evento. In tal modo, tuttavia, si verrebbe a perdere non soltanto il nesso di tipo soggettivo con il risultato, ma financo l'azione medesima, giacché sarebbe comunque assente – *ex ante* – una valida regola cautelare che avrebbe dovuto essere rispettata dall'agente. La "colpa eventuale", dunque, diverrebbe «uno strumento di impropria criminalizzazione, diretto a fronteggiare (al pari di una terapia farmacologica od anestetica collettiva) l'*epistemologia dell'incertezza*, nonché a tacitare di volta in volta le richieste di tutela emergenti dal corpo sociale o, addirittura, le fobie e paranoie collettive» (p. 209). L'asse del disvalore tenderebbe così a scivolare sul versante del *tipo d'autore*: autore punito come «capro espiatorio», non tanto per aver cagionato "personalmente" un danno, ma soltanto per la rivestita "posizione di prossimità" rispetto al processo di implementazione, nella vita della società, di un rischio tecnologico mai davvero accettato e "digerito" dai consociati. Sullo "svuotamento" delle categorie tradizionali di imputazione del reato d'evento, in contesto di ignoto tecnologico, cfr. anche, per tutti, Stortoni (2004), pp. 74 ss. infine, Piergallini (2017), pp. 247-248, sottolinea più in generale l'arretratezza della nozione giurisprudenziale di colpa rispetto alle elaborazioni della dottrina.

[71] Così descrive Piergallini (2004), pp. 440 ss., nonché più in breve Piergallini (2007), p. 1128, sottolineando peraltro sempre con forza come tali meccanismi imputativi utilizzati dalle corti forzino indebitamente la tipicità sia oggettiva che soggettiva dell'illecito colposo d'evento.

[72] Per tutti, sul *machine learning* nell'*autonomous driving*, Stilgoe (2018). Cfr. anche Surden e Williams (2016), pp. 147 ss., 162-163, e più in generale sul *machine learning* in ambito giuridico v. Surden (2014).

[73] Per tutti, Gless *et al.* (2016), p. 414, Beck S. (2016), p. 140, Beck S. (2017), p. 243.

box, proprio a indicare l'opacità dei processi decisionali che avvengono dentro la macchina.

Di fronte a tale scenario, dunque, si comprende ancor più perché sia difficile individuare – a monte – un singolo errore del programmatore, che abbia con certezza causato un certo comportamento dell'auto, e conseguentemente un certo danno. Vi sono casi in cui un qualunque giudizio di prevedibilità *ex ante* è puntualmente destinato a naufragare, minando così qualsivoglia prospettiva di imputare per colpa quel fatto a un soggetto umano. E comunque, in base al principio dell'oltre ogni ragionevole dubbio, anche tutti quei casi in cui non sia certa la natura del malfunzionamento devono necessariamente essere ricondotti alla più favorevole ipotesi del "fatto proprio" dell'intelligenza artificiale, ovvero della sua non imputabilità a soggetti umani.

Residua dunque, nelle auto completamente autonome, *un ventaglio di casi in cui il danno rimane sostanzialmente (o presuntivamente) riconducibile alla macchina stessa*: casi, pertanto, irrimediabilmente destinati a rimanere penalmente irrilevanti[74]. Questo inquietante vuoto di responsabilità ci sembra essere l'area più problematica da gestire sotto un profilo politico-criminale, nell'ottica di allocazione di tale rischio tecnologicamente derivato.

Questo rischio ricade, anzitutto, sulla vittima. Infatti, se nessuno è additabile come responsabile è proprio quest'ultima l'unica a "pagare" per un fatto che potrebbe sembrare sostanzialmente imputabile al caso, alla sorte avversa. Ma in realtà il rischio in questione è diverso rispetto a quanto accade per le fatalità naturali, non prevedibili o non impedibili da parte dell'uomo, nella misura in cui esso è *creato* dall'uomo e dallo stesso *tollerato*, in base a un giudizio di valore che stimi socialmente prevalente l'interesse a giovarsi dei benefici derivanti dall'uso della tecnologia *driverless*[75].

Un bilanciamento in questo senso, certamente, permetterebbe di salvare molte vite che in mancanza dell'*autonomous driving* sarebbero andate perdute: numericamente ben di più di quelle "sacrificate" pur di consentire l'utilizzo di tale tecnologia. È innegabile, tuttavia, il fatto che *quelle specifiche, concrete vittime* ricadrebbero sulle spalle della società intera, che ha compiuto una precisa e consapevole scelta politica di barattare la loro incolumità con quella della più ampia moltitudine che, in tal modo, viene risparmiata[76].

Nessun altro modo di proteggersi da tali rischi imprevedibili ma ineliminabili esiste se non attraverso l'opposta scelta di proibire l'*autonomous driving*, appellandosi ancora a istanze di precauzione[77]. In tal caso, il rischio in questione verrebbe stimato come non tollerato, di talché l'unica regola cautelare possibile di fronte a esso sarebbe l'obbligo di astenersi da tale attività. Ma ogni beneficio derivante da tale tecnologia – è evidente – sarebbe così precluso[78].

In sintesi, si potrebbe dire che una volta *scomparsa la figura del conducente ad assorbire, suo malgrado, l'intima contraddizione tra due esigenze tra loro inconciliabili, la tensione tutta politica tra vantaggi sociali e istanze precauzionistiche si presenta nella sua nudità*. L'alternativa è secca: autorizzare e accettare che i beni in gioco possano in taluni casi concreti rimanere scoperti da tutela; o proibire, perdendo però a livello globale i benefici, anche in termini di vite umane, di tale nuova tecnologia.

È molto difficile prevedere come la tensione descritta verrà risolta, in scenari sociali, politici e anche tecnologici tutto sommato ancora abbastanza lungi dal venire a esistenza. Probabilmente, si rivelerà pervicace e duratura la resistenza ad autorizzare veicoli completamente *driverless* nel nostro paese, come negli altri ordinamenti europei. L'affidarsi completamente a una macchina, senza lo schermo rassicurante (benché fittizio) della responsabilità del "conducente potenziale", evoca timori dell'ignoto difficili da governare con razionalità, e che – si

[74] Beck S. (2017), p. 243 ss., nonché Gless *et al.* (2016), p. 432, che parlano proprio di "*responsibility gap*".
[75] Cfr. Gless *et al.* (2016), pp. 430 ss.
[76] Ma osservano giustamente – in campo etico – Hevelke e Nida-Rümelin (2015), p. 623, che per *qualunque* misura di sicurezza ci possono essere dei casi concreti in cui essa faccia «più male che bene»; o addirittura sia causa di un danno, che in sua assenza non si sarebbe verificato. Si consideri, ad esempio, la cintura di sicurezza, per rimanere nell'ambito della circolazione stradale. Se di normale essa costituisce un presidio capace di ridurre i danni alle persone, in casi eccezionali può bloccarsi e imprigionare così i passeggeri, esponendoli senza possibilità di fuga alle fiamme di un incendio, o all'affogamento dentro il veicolo che affondi. Tuttavia, certamente «questi tragici casi non cambiano il fatto che tali misure innalzino significativamente la sicurezza complessiva» degli utenti della strada.
[77] Per tutti, già Stortoni (2004), p. 83, nonché più specificamente Beck S. (2017), p. 243.
[78] Gless *et al.* (2016), p. 430.

immagina – occorrerà tempo per fugare[79]. È a nostro giudizio auspicabile, tuttavia, che prevalgano infine istanze di tolleranza del pericolo tecnologico, facendo ricadere tale ineliminabile sacca di imprevedibilità nell'orbita del rischio consentito[80].

In effetti, una volta razionalizzata a livello antropologico e culturale l'esistenza di questo "vuoto", l'esigenza di soddisfare le pur legittime pretese delle vittime può essere forse ricondotta a piani diversi da quello penalistico, primo fra tutti quello risarcitorio[81]: che consentono degli schemi imputativi che, in ipotesi eccezionali, prescindano dai principi – invece irrinunciabili per il diritto penale – di responsabilità per fatto proprio e colpevolezza.

6. *Autonomous driving* e reati stradali in senso stretto.

Esaurito il più complesso tema del reato colposo d'evento, è adesso possibile concentrarsi sui riflessi dell'*autonomous driving* rispetto ai reati stradali in senso stretto. Il riferimento, qui, è a gli illeciti volti a tutelare la sicurezza stradale previsti dal Codice della strada, con cui sono penalmente sanzionate alcune fra le più pericolose condotte di guida – o prodromiche alla guida – proprio in ragione della loro rischiosità[82].

È un tema, questo, che forse può apparire più scontato o meno interessante del precedente, ma che è necessario sia pur brevemente considerare per esigenze di completezza. Del resto, è ben vero che nel sistema italiano la tutela penale della sicurezza stradale si radica molto di più sul versante del reato tradizionale d'evento che su fattispecie di pericolo a carattere anticipato. Il versante della prevenzione, nel nostro ordinamento, è lasciato in larga parte a sanzioni di tipo amministrativo. Ciò differisce fortemente da altri sistemi – ad esempio, quello spagnolo – dove si è preferito incentrare la tutela penale della sicurezza stradale sulla repressione di condotte pericolose soltanto prodromiche all'offesa effettiva, peraltro sanzionate in maniera anche piuttosto significativa[83].

La rivoluzione dell'*autonomous driving*, ci sembra, prospetta scenari differenziati di adattamento dei vari reati del Codice della strada che ci accingiamo adesso a prendere in considerazione. Più in particolare, tali illeciti meritano di essere brevemente analizzati in via separata, basandosi proprio sugli *effetti* che la nuova tecnologia provocherebbe su di loro.

Muoviamo anzitutto dai reati connessi alle gare clandestine: i comportamenti di chi in vario modo organizzi una competizione in velocità non autorizzata, oppure la condotta di intraprenderla concretamente su strada, senza previa organizzazione, previsti e puniti rispettivamente dagli artt. 9 *bis* e 9 *ter* del Codice della strada[84].

Rispetto a essi, è sostanzialmente la stessa "ontologia" del concetto di competizione a sembrare incompatibile con la tecnologia di guida autonoma. L'idea medesima di gara, anzitutto, pare inestricabilmente connessa con le capacità individuali al volante, che sono invece "livellate" dall'*autonomous driving*. E comunque nessuna *self-driving car* legale sarà mai programmata per poter essere utilizzata in una gara, anzi – lo abbiamo già detto – salvo situazioni di emergenza l'intelligenza artificiale alla guida non potrà neanche superare i limiti di velocità consentiti. Se qualcuno intende partecipare a una competizione, continuerà ovviamente a usare un'auto tradizionale; o, al massimo, una vettura semi-autonoma, che potrà sempre essere

[79] Si rinvia ancora alle profonde riflessioni riguardo l'«illusione prometeica» circa le possibilità di controllo del caso fortuito da parte della tecnica svolte da Castronuovo, (2009), pp. 92 ss.

[80] Così sostanzialmente anche Gless *et al.* (2016), pp. 433 ss.

[81] Secondo tradizionali meccanismi assicurativi di riallocazione dei risarcimenti sull'intera platea degli utenti della strada, che *prima facie* paiono meno problematici rispetto all'imputazione penalistica dei fatti, magari coadiuvati da fondi pubblici di risarcimento per le vittime da attivare nei casi problematici, da finanziare ricorrendo alla fiscalità generale.

[82] Si possono indicare come riferimenti generali, per tutti: Pavich e Sturlese (2018), Piccioni (2017), Reccia (2014), pp. 4 ss., Forlani e Planitario (2013), pp. 67 ss., Riccardi (2010), pp. 6 ss., Musacchio (2007), in particolare pp. 91 ss. In ambito statunitense, v. Gurney (2015), pp. 412 ss., nonché Palodichuk (2015), pp. 829 ss.

[83] Si fa qui riferimento, in particolare, ai *delitos contra la seguridad vial* di cui agli artt. 379 ss. del *código penal*, su cui, per tutti, v. dettagliatamente De Vicente Martínez (2008), pp. 297 ss., o più succintamente Cancio Meliá e Llobet Anglí (2014). Per un panorama dei reati stradali in vari altri paesi europei (Olanda, Inghilterra e Galles, Francia e Germania) si vedano gli ulteriori contributi del volume collettaneo Van Dijk e Wolswijk (eds.) (2014).

[84] Su tali reati, per tutti: Pavich e Sturlese (2018), pp. 24 ss., Piccioni (2017), pp. 29 ss. e 105 ss.

manualmente lanciata a qualunque velocità che il mezzo possa tecnicamente sostenere.

Così, criminologicamente parlando, chi vuol organizzare o partecipare a gare clandestine verosimilmente non si accorgerà nemmeno della transizione tecnologica. Similmente, chi verrà "sfidato" al semaforo dal rombo del veicolo che si sia affiancato potrà continuare, come in precedenza, ad accettare la provocazione; sempreché non si trovi su una vettura completamente autonoma. Ma in tal caso, magari, neanche si accorgerà della sfida lanciatagli, preso a fare tutt'altro…

Un altro gruppo di illeciti da considerare sono i delitti consistenti nella violazione dell'obbligo di fermata e soccorso ai feriti in caso di incidente con danni a persone, di cui all'art. 189, commi 6 e 7, del Codice della strada[85].

Rispetto a tali reati, ci sembra che l'impatto dell'*autonomous driving* sia sostanzialmente irrilevante, dato che l'obbligo di fermata e soccorso del conducente pare scattare in ogni caso, indipendentemente dal tipo di vettura in discussione. Addirittura, la formulazione molto ampia dell'art. 189 C.d.s. potrebbe essere intesa nel senso che tale obbligo gravi anche sul mero occupante-passeggero di un mezzo completamente autonomo. Né, dal punto di vista pratico, la natura automatizzata del veicolo impedisce il dispiegarsi dell'obbligo di fermata e soccorso, differentemente da quanto accade con gli obblighi di sorveglianza dell'attività della vettura. Anche se non ci sono volante né pedali per poter guidare, il passeggero avrà pur sempre il potere di selezionare o mutare la destinazione, oppure di far fermare il mezzo, in un qualunque momento. La natura autonoma del veicolo, poi, non è tale da impedire all'occupante di accorgersi della situazione concretamente realizzatasi. Il presupposto dei reati in questione è infatti l'avvenuta verificazione di un incidente a sé ricollegabile[86]: un sinistro che dunque inevitabilmente coinvolga anche la vettura autonoma medesima.

Scappare premendo l'acceleratore, oppure scappare ordinando alla *self-driving car* di farlo, sempre di fuga si tratta. Non pare, dunque, che rispetto a questi illeciti – tutto sommato neanche in una prospettiva *de jure condendo* – l'*autonomous driving* possa mutare qualcosa rispetto a quanto l'esperienza attuale già conosce.

Rimangono infine da affrontare i reati stradali più significativi, non soltanto dal punto di vista statistico: ovvero quelli relativi alla guida sotto l'influenza dell'alcool o in stato di alterazione psico-fisica connesso all'uso di sostanze stupefacenti, *ex* artt. 186, 186 *bis* e 187 del Codice della strada[87].

Già si è detto come uno dei benefici possibili della guida autonoma è proprio quello di prevenire il fenomeno del *drunk driving* e i connessi rischi per la sicurezza stradale[88]. Tuttavia, la previsione di pulsanti del genere "*Take me home, I'm drunk*"[89] creerebbe significativi problemi a livello regolativo. Solo nelle vetture completamente autonome, infatti, in cui l'occupante sia sollevato da ogni obbligo di controllo, potrà davvero esistere un comando di questo tipo. Rispetto a tali ipotesi, i reati in discussione sono dunque evidentemente destinati a non essere più applicabili[90].

Ma nelle vetture semi-autonome, e comunque nella misura in cui il legislatore, pur autorizzando l'*autonomous driving*, continuerà a imporre al "conducente" un obbligo di sorveglianza del mezzo durante le fasi di crociera, la perdita di reattività connessa all'uso di alcool o sostanze stupefacenti sarebbe comunque fonte di un rischio non consentito[91]. Anche se nella

[85] Rispetto a tali illeciti, per tutti: Pavich e Sturlese (2018), pp. 225 ss., Piccioni (2017), pp. 313 ss.

[86] Cfr. art. 189, comma primo, C.d.s.

[87] Su tali illeciti, v. a livello monografico Scotti (2016), e Cirillo (2012), oltre alle trattazioni di Pavich e Sturlese (2018), pp. 76 ss., Piccioni (2017), pp. 117 ss., e Reccia (2014), pp. 4 ss.

[88] Sull'intersezione tra *autonomous driving* e *drunk driving*, in generale, v. Hanna (2015), Gurney (2015), pp. 419 ss. e Tranter (2016), pp. 69 ss.

[89] Lo immaginano Douma e Palodichuk (2012), p. 1158, che pure più avanti (pp. 1163-1164) si rendono conto della sua problematicità.

[90] Hanna (2015), pp. 282 e 286-287.

[91] Douma e Palodichuk (2012), p. 1163, Gurney (2015), p. 420, Tranter (2016), pp. 70-71. Hanna (2015), p. 288, propone in alternativa di rendere obbligatoria l'implementazione di comandi con cui, al momento della partenza, il passeggero segnali al mezzo di non essere capace di gestire le situazioni di emergenza, obbligando quest'ultimo – al presentarsi di tali casi – di fermarsi. Ma non sempre, si potrebbe obiettare, le situazioni di emergenza sono riconosciute dal veicolo autonomo come tali, né sempre è possibile risolverle mediante l'arresto della corsa (magari impossibile nella circostanza concreta).

quasi totalità dei casi il concreto stato di alterazione del "conducente" non sarebbe pericoloso, giacché la macchina farebbe tutto da sola senza necessità di interventi umani, in caso di malfunzionamento del mezzo verrebbe tuttavia meno, o comunque sarebbe pregiudicata nelle sue capacità, la doverosa figura di garanzia umana. Il risultato è dunque paradossale dal punto di visto politico-criminale. Da un lato, è ben vero che il permettere il *drunk driving* nelle vetture semi-autonome farebbe calare di molto le percentuali dei sinistri[92]. Dall'altro, tuttavia, una simile autorizzazione si porrebbe in logica incompatibilità con l'imposizione, in generale, di un obbligo di controllo in capo al conducente. Tale obbligo, in pratica, verrebbe assurdamente meno solo nella circostanza – peraltro giuridicamente riprovata – del *drunk driving* medesimo.

Sembra dunque ineludibile, dal punto di vista politico-criminale, una soluzione nel senso di criminalizzare le condotte di sorveglianza di una *semi-autonomous car* in stato di intossicazione, parificandole alla guida tradizionale sotto l'effetto di alcool o droghe. È comunque dubbio se le attuali fattispecie di cui agli artt. 186 e seguenti del Codice della strada possano essere lette in tal senso, o se, per giungere a un simile risultato, sarebbe necessario un intervento *ad hoc*[93]. Tali reati, infatti, non si imperniano sull'elastica figura attiva del "conducente", che più facilmente si presta a interpretazioni in senso estensivo, quanto piuttosto sulla condotta vincolata del "guidare", a cui con più difficoltà sembra riconducibile quella di mera sorveglianza del funzionamento della vettura autonoma[94].

7. Nuove fenomenologie criminali e nuove esigenze di tutela: in particolare, il nodo della *cybersecurity*.

Se finora ci si è interrogati circa la compatibilità con l'*autonomous driving*, e i necessari adattamenti, dei tradizionali reati connessi alla circolazione stradale, è infine opportuno chiedersi se da tale tecnologia non emergano inedite esigenze di tutela che necessitano di essere affermate mediante l'introduzione di nuove fattispecie penali[95].

L'operazione in questione non è affatto semplice, dal momento che sostanzialmente essa consisterebbe nel cercare di trarre delle conseguenze sul piano penalistico, muovendo da mere ipotesi relative alle modalità di sviluppo dei fenomeni criminosi connessi alla diffusione della guida autonoma. Essa, dunque, sconta un profilo doppiamente ipotetico: sia, come detto, in ordine al contesto criminale considerato; sia in ordine alla futuribile normativa – non necessariamente penalistica – che potrà essere adottata per farvi fronte. Ci limiteremo, pertanto, a procedere per aree tematiche in modo meramente esemplificativo, senza la minima pretesa di esaustività.

Un primo settore che potrebbe essere toccato dall'*autonomous driving* è quello dei traffici, in particolare di stupefacenti. Un veicolo completamente autonomo privo di occupanti, è stato fatto notare, potrebbe efficacemente svolgere un ruolo di "corriere robotico" di droga o

[92] Hanna (2015), p. 281. Il parametro di riferimento, ovviamente, è rispetto alle auto tradizionali, a numero invariato di conducenti alterati. Gurney (2015), p. 422-423, auspica conseguentemente che, raggiunto un certo livello di sicurezza dell'*autonomous driving*, il legislatore renderà lecito il *drunk driving* nei veicoli semi-autonomi.

[93] Per una analisi della questione in ambito statunitense v. Hanna (2015), pp. 286 ss.

[94] Dei reati previsti dal Codice della strada – oltre a quello di falsificazione di targhe *ex* art. 100, comma 14, C.d.s., evidentemente estraneo alla tutela della sicurezza stradale – non si è detto del reato di *guida senza patente*, trasformato in illecito amministrativo dal d. lgs. 8/2016 nella sua ipotesi base di cui all'art. 116, comma 15, C.d.s., ma ancora perseguito penalmente in caso di recidiva nel biennio e nell'ipotesi speciale di cui all'art. 73 del Codice antimafia (sebbene quest'ultima sia ritenuta tutelare non la sicurezza stradale ma l'ordine pubblico). Su tale reato, per tutti, cfr. Pavich e Sturlese (2018), pp. 57 ss., Piccioni (2017), pp. 85 ss. Per quanto attiene l'impatto dell'*autonomous driving* su tale illecito, potrebbe dirsi che vale un ragionamento simile a quanto compiuto rispetto ai reati di guida sotto l'effetto di alcool o stupefacenti. Nelle auto completamente autonome, infatti, non ha senso alcuno parlare di guida senza patente, giacché una delle funzioni di tali mezzi sarebbe proprio quella di mobilizzare persone prive di patente o comunque impossibilitate a guidare. Nelle vetture semi-autonome, invece, fintantoché il conducente potenziale ha l'obbligo di sorvegliare il mezzo e di intervenire in caso di bisogno è necessario che abbia la patente, di talché il reato sarà integrabile.

[95] Risposta – lo si anticipa – a nostro avviso negativa per il futuro prossimo, come ritenuto anche da Hilgendorf (2017), p. 181. *Contra*, invece, Glancy (2015), pp. 663-664 e Palodichuk (2015), p. 831.

di altri prodotti illeciti, eliminando la figura del corriere come oggi la conosciamo, la quale è solitamente il punto di inizio delle indagini in materia di traffici[96]. Certo, in sua assenza ci sarebbe comunque un primo sospettato, ovvero il proprietario del mezzo. Ma la vettura potrebbe essere rubata: e qui si entrerebbe in un secondo possibile ambito criminoso, quello dei furti e delle ricettazioni d'auto. Si renderebbe necessario, così, prevedere dei sistemi che permettano al proprietario di bloccare l'auto a distanza, oppure di tracciarla ovunque sia[97], oppure ancora imporre delle scatole nere obbligatorie, che registrino la provenienza del veicolo e la destinazione impostata[98]. Ma queste ipotesi, ancora, sarebbero probabilmente discutibili sul piano della tutela della *privacy*.

Insomma, già da questi esempi, si può notare come la tecnologia *driverless* necessiterà di valutazioni complesse circa le differenti possibili soluzioni regolative da adottare. Non ci sembra, però, che queste chiameranno davvero in causa il diritto penale sostanziale. Le fattispecie a venire in gioco, in simili future e ipotetiche fenomenologie di traffici criminosi, sarebbero infatti le stesse già previste oggi: soltanto, potrebbero mutare le modalità con cui tali reati verranno realizzati. I problemi che queste fenomenologie potrebbero porre, piuttosto, riguarderanno dunque sostanzialmente delle difficoltà inedite sul piano delle indagini.

Considerazioni simili potrebbero essere fatte anche rispetto ad altri fenomeni criminosi. Per tutti, si è evidenziato come vetture completamente autonome potrebbero essere usate per commettere reati contro l'incolumità pubblica e di terrorismo[99]. Alle già note metodologie d'attentato del camion-bomba parcheggiato presso obiettivi sensibili e del veicolo *kamikaze*, si aggiungerebbe quello della vettura "esplosiva" a guida autonoma, che permetterebbe di unire i vantaggi della mobilità del mezzo a quello della non necessaria immolazione del terrorista[100].

Ma anche qui, ci pare, l'aggravio di pericolosità prospettato da questa fenomenologia potrebbe essere meglio fronteggiato a livello extrapenale che penalistico[101]. Del resto, sarebbe arduo individuare condotte prodromiche specifiche da criminalizzare, dotate dei crismi dell'inequivocità e dell'idoneità, che sfuggano al già sviluppatissimo e reticolare paradigma di criminalizzazione anticipata, così tipico di quelle classi di reati.

L'ambito criminoso più delicato e interessante, tuttavia, è probabilmente quello connesso alla *cybersecurity* delle macchine a guida autonoma[102].

Già adesso, le auto in commercio – in cui ogni funzione è ormai controllabile dall'elettronica integrata del mezzo – sono attaccabili da parte di *hacker* che operino dall'esterno, da remoto. Le vie d'ingresso che questi ultimi sfruttano sono i possibili "buchi" in quei programmi che consentono alle vetture di collegarsi *wireless* allo *smartphone* del conducente, permettendogli, ad esempio, di effettuare chiamate, impostare il navigatore, o altre funzioni ancora. Alcuni esperimenti hanno mostrato come in tal modo l'*hacker* sia in grado di prendere il controllo sostanzialmente totale del mezzo, incluse funzioni basilari quali lo spegnimento del motore e il comando dei freni[103].

Tali a dir poco inquietanti profili di rischio sono evidentemente destinati ad amplificarsi a dismisura se coniugati con tecnologie di guida autonoma. L'attacco informatico, infat-

[96] Douma e Palodichuk (2012), pp. 1165-1166.

[97] Un po' come già avviene per certi dispositivi tecnologici connessi alla rete o localizzabili tramite GPS, quali *smartphones* o *tablets*.

[98] Paiono suggerirlo Douma e Palodichuk (2012), p. 1166.

[99] Lewis (2015), Douma e Palodichuk (2012), pp. 1166-1167. Addirittura l'FBI ha prospettato il rischio che le *autonomous cars* possano facilitare atti di terrorismo: Harris (2014).

[100] Appaiono difficili, invece, attentati sul modello del mezzo lanciato sulla folla in costanza di grandi eventi, quali si sono ripetutamente verificati in Europa negli ultimissimi anni. Il mezzo autonomo, infatti, di norma non potrà violare le norme del Codice della strada, e non può essere impostato per investire qualcuno. Differente è il caso della vettura oggetto di *hacking*, per la quale l'aggressione informatica potrebbe (forse) addirittura riuscire a sovrascrivere queste impostazioni algoritmiche di sicurezza di base.

[101] Alcune soluzioni sono proposte da Douma e Palodichuk (2012), pp. 1166-1167.

[102] Sul tema, Allison (2016), Wing (2016), Lee (2017), Kennedy (2017), Douma e Palodichuk (2012), pp. 1164-1165, Tranter (2016), pp. 75 ss., o più in generale Suchodolski (2018). Quello dei possibili sabotaggi informatici, secondo Hilgendorf (2017), p. 175, è il maggiore problema connesso all'*autonomous driving*.

[103] Nell'episodio con maggiore eco mediatica, due esperti di sicurezza erano riusciti a prendere il controllo della jeep di un giornalista, addirittura facendola finire fuori strada: Greenberg (2015). Più in generale, per una «*Brief History of Car Hacking*», Allison (2016), pp. 17 ss.

ti, potrebbe anzitutto permettere all'*hacker* l'accesso a informazioni riservate dell'utente, con pregiudizio della *privacy*[104]. Ma è la sicurezza stradale il bene più significativo che sarebbe davvero minacciato ove il mezzo ricadesse nell'integrale disponibilità del criminale[105]. Gli effetti potrebbero variare dal tenere imprigionato l'occupante del veicolo, all'ucciderlo in un sinistro appositamente provocato, o addirittura all'utilizzare la vettura come arma per provocare un incidente coinvolgente anche terzi. Se poi si considera il fatto che le *self-driving cars* più avanzate in futuro potrebbero "parlare" tra di loro in *cloud*, sfrecciando ravvicinate grazie al coordinamento artificiale del traffico, ben si capisce come l'*hacking*, anche solo di un mezzo, potrebbe permettere di compiere dei veri e propri attentati "cyberterroristici" su larga scala[106].

Dal punto di vista penalistico è chiaro come la condotta di intrusione nel sistema informatico di una *autonomous car* integrerebbe già gli estremi dell'accesso abusivo a sistema informatico, di cui all'art. 615 *ter* c.p.[107]. Ci si potrebbe chiedere, tuttavia, se la particolare gravità degli effetti che possono derivarne, e quindi la peculiare pericolosità della condotta di *hacking* di vetture a guida autonoma, possa giustificare la creazione legislativa di una fattispecie *ad hoc*, più grave, che incrimini il "dirottamento informatico" di una *self-driving car*[108].

Ci sembra, tuttavia, che la fenomenologia in questione – pur, ovviamente, futura e quindi ancora del tutto ipotetica – indicherebbe piuttosto l'urgenza di intraprendere scelte regolative di tipo differente. L'esperienza in materia di *cybercrime*, infatti, mostra come sia davvero difficile, se non quasi impossibile, individuare e perseguire gli autori delle condotte di *hacking*, sovente incuranti dei confini nazionali, con gli strumenti dell'ordinamento penale. Piuttosto, la priorità dovrà essere accordata alla difesa rispetto tali condotte e alla *prevenzione* dei danni, mediante l'implementazione di una serie di standard in materia di *cybersecurity*.

Si possono fare alcuni esempi. In primo luogo, la previsione di un obbligo per il sistema del veicolo autonomo di effettuare dei controlli periodici su sé stesso, al fine di individuare eventuali anomalie o interferenze esterne, rilevate le quali dovrebbe immediatamente prodursi il blocco del veicolo. O ancora, l'imposizione di una struttura del sistema informatico del mezzo quanto più possibile a "compartimenti stagni", in modo da consentire di isolare, in caso di emergenza, l'intrusione esterna, e comunque di ostacolarne la presa di controllo totale del mezzo. Infine, la previsione che nelle auto semi-autonome la guida manuale "sovrascriva" sempre qualsivoglia comando impartito dal veicolo stesso; e comunque, in ogni mezzo, la possibilità di arrestare il veicolo manualmente in ogni momento, oltre alla previsione di meccanismi manuali di apertura delle portiere, che l'intelligenza artificiale della vettura non possa mai disabilitare[109].

---

[104] Per tutti, Lee (2017), pp. 31 ss. e Wing (2016), pp. 727.

[105] Per cui l'*hacker* sarebbe responsabile per tutti i reati dolosi derivanti dalla propria condotta, come l'omicidio. Cfr. Tranter (2016), p. 75, Gurney (2015), pp. 429, 433 ss., Wing (2016), p. 725, con riferimento al reato di *kidnapping*. Evidenzia Hilgendorf (2017), pp. 182-183, come peraltro in tali casi non sia soltanto l'*hacker* a incorrere in responsabilità penali, ma possono venire in gioco anche le figure del *programmatore* e dell'*installatore* dei sistemi di *cybersecurity*, ove un loro errore o mancanza sia causalmente riconducibile all'accesso abusivo del criminale informatico (sempreché la causazione dell'evento finale – evidentemente – sia sanzionata anche a titolo colposo).

[106] Wing (2016), pp. 729 ss.

[107] O anche del delitto di diffusione di programmi nocivi di cui all'art. 615 *quinquies* c.p. nel caso in cui l'*hacker* aggredisca il sistema informatico della vettura autonoma con un *malware*. Il concorso dai due delitti è ammesso in giurisprudenza ma tendenzialmente negato dalla dottrina. In merito a questo tema si rinvia a Cappellini (2019b), pp. 817-818. In ambito federale statunitense, come segnalato da Gurney (2015), pp. 438 ss., similmente tali condotte sarebbero punite in base al CFAA (*Computer Fraud and Abuse Act*).

[108] Ci pare, invece, che *de jure condito* sia insostenibile l'applicabilità del reato di furto, se non addirittura di rapina, per i casi di *hacking* del mezzo, quantomeno nella loro forma consumata. Potrebbe infatti forse ritenersi che la presa del controllo del veicolo equivalga ad una "sottrazione", così come che la soggezione del "conducente" alla volontà dell'*hacker* nel controllo della vettura sia qualificabile come violenza personale fisica impropria (cfr. per tutti, su tale concetto, Mantovani F. (2011), pp. 264-265). Ma certamente pare difficile affermare che si è realizzato l'elemento di fattispecie dell'"impossessamento" fintantoché la macchina non sia uscita dalla sfera di controllo del proprietario, che invece persiste se quest'ultimo rimane fisicamente presente dentro al mezzo. In ambito statunitense, Douma e Palodichuk (2012), p. 1165 propongono invece la riconducibilità in via analogica dell'*hacking* al *theft* di auto, o addirittura al *carjacking* – ovvero la condotta di prendere il possesso di una vettura con violenza personale. Gurney (2015), p. 438, esclude invece la configurabilità del *carjacking* a livello federale. Wing (2016), pp. 739 ss., infine, propone la formulazione proprio di un reato federale consistente nell'«*Hacking an autonomous vehicle*».

[109] Esempi di tale misure di sicurezza sono proposti da Lee (2017), pp. 49 ss., e Kennedy (2017), pp. 347 ss.

Risultati soddisfacenti potrebbero forse essere raggiunti già mediante meccanismi di autoregolamentazione da parte delle case automobilistiche stesse, nello sforzo di promuoversi sul mercato agli occhi degli utenti[110]. Tuttavia, è indubbio come l'entità dei beni minacciati imponga una regolamentazione da parte dell'ordinamento, tesa a fissare degli standard minimi in tema di *cybersecurity*, per quanto riguarda le *self-driving cars*: ma, in fondo, anche per le vecchie auto tradizionali, che come si è visto non sono esenti da pericoli[111].

Bibliografia

Addante, Eleonora (2017): "*Vox populi vox Dei?* L'omicidio stradale: una riforma figlia del tempo attuale": *Archivio Penale Web*, 2, pp. 1-32.

Allison, Liz (2016): "You Can't Hank This: The Regulatory Future of Cybersecurity in Automobiles", *Journal of Technology Law & Policy*, 21, pp. 15-35.

Aria, Erfan, Olstam, Johan, Schwietering, Christoph (2016): "Investigation of Automated Vehicle Effects on Driver's Behaviour and Traffic Performance", *Trasportation Research Procedia*, 15, pp. 761-770.

Asaro, Peter M. (2012): "A Body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics", in Lin, Patrick, Abney, Keith, Bekey, George A. (eds.), *Robot Ethics* (Cambridge-Massachusetts, MIT Press), pp. 169-186.

Beck, Susanne (2017): "Google Cars, Software Agents, Autonomous Weapons Systems – New Challanges for Criminal Law", in Hilgendorf, Eric e Seidel, Uwe (eds.), *Robotics, Autonomics and the Law* (Baden-Baden, Nomos), pp. 227-251.

Beck, Susanne (2016): "Intelligent agents and criminal law – Negligence, diffusion of liability and electronic personhood", *Robotics and Autonomous Systems*, 86, pp. 138-143.

Beck, Ulrich (1986): *Risikogesellschaft. Auf dem Weg in eine andere Moderne* (Frankfurt, Suhrkamp); in traduzione italiana (2000): *La società del rischio. Verso una seconda modernità* (Roma, Carocci).

Beiker, Sven A. (2012): "Legal Aspects of Autonomous Driving", *Santa Clara Law Review*, 52, pp. 1145-1156.

Bianchi, Davide (2016): "I nuovi delitti di omicidio e lesioni stradali (commento alla l. 23 marzo 2016, n. 41)", *Studium Iuris*, 6, pp. 679-685.

Bonnefon, Jean-François, Shariff, Azim, Rahwan, Iyad (2016): "The social dilemma of autonomous vehicles", *Science*, 352 (6293), pp. 1573-1576.

Butti, Luciano (2016): "Auto a guida autonoma: sviluppo tecnologico, aspetti legali ed etici, impatto ambientale", *Rivista Giuridica dell'Ambiente*, 3/4, pp. 435-452.

Cancio Meliá, Manuel e Llobet Anglí, Mariona (2014): "The Spanish Perspective on Traffic Offences: Tough on Danger, Soft on Harm, and Penal Populism", in Van Dijk, Alwin e Wolswijk, Hein (eds.), *Criminal Liability for Serious Traffic Offences* (The Hague, Eleven), pp. 107-130.

Cappellini, Alberto (2019a): "*Machina delinquere non potest?* Brevi appunti su intelligenza artificiale e responsabilità penale", *Criminalia*, 12 (2018), pp. 155-176 (in pubblicazione); anticipato sul portale *DisCrimen* il 27.3.2019.

[110] È la prospettiva promossa da Allison (2016), pp. 28 ss., che si appella al precedente dell'autoregolamentazione del mercato in materia di standard di sicurezza per i pagamenti con carte di credito.
[111] Tale è invece l'idea – in ambito USA – di Lee (2017), pp. 43 ss. Kennedy (2017), pp. 353 ss., evoca addirittura l'idea di una *cyberinsurance* e della creazione di un fondo federale per le vittime di *hacking* veicolare.

Cappellini, Alberto (2019b): "I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici", in Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo, Papa, Michele (eds.), *Cybercrime* (Milano, UTET-WKI), pp. 761-826.

Cappellini, Alberto (2017): "Circolazione stradale e principio di affidamento: l'impervio cammino della personalizzazione dell'illecito colposo", *Parola alla Difesa*, 6, pp. 643-655.

Castronuovo, Donato (2012): *Principio di precauzione e diritto penale: paradigmi dell'incertezza nella struttura del reato* (Roma, Aracne).

Castronuovo, Donato (2009): *La colpa penale*, (Milano, Giuffrè).

Castronuovo, Donato (2005): "Responsabilità da prodotto e struttura del fatto colposo", *Rivista Italiana di Diritto e Procedura Penale*, 301-340.

CB Insight (2018): "46 Corporations Working on Autonomous Vehicles", https://www.cbinsights.com/research/autonomous-driverless-vehicles-corporations-list/ , pubblicato il 4.9.2018, ultimo accesso il 5.3.2019.

Cirillo, Bruno (2012): *Guida in stato di alterazione da alcool o sostanze stupefacenti* (Milano, Giuffrè).

Civello, Gabriele (2013): *La "colpa eventuale" nella società del rischio. Epistemologia dell'incertezza e "verità soggettiva" della colpa* (Torino, Giappichelli).

Coca-Vila, Ivó (2018): "Self-driving Cars in Dilemmatic Situations: An Approach Based on the Theory of Justification in Criminal Law", *Criminal Law and Philosophy*, 12, pp. 59-82.

Coca-Vila, Ivó (2017): "Coches autopilotados en situaciones de necesidad. Una aproximación desde la teoría de la justificación penal", *Cuadernos de Política Criminal*, 122, II, pp. 235-275.

Contissa, Giuseppe, Lagioia, Francesca, Sartor, Giovanni (2017a): "The Ethical Knob: ethically-customisable automated vehicles and the law", *Artificial Intelligence and Law*, 25, pp. 365-378.

Contissa, Giuseppe, Lagioia, Francesca, Sartor, Giovanni (2017b): "La manopola etica: i veicoli autonomi eticamente personalizzabili e il diritto", *Sistemi Intelligenti*, 3, pp. 601-614.

Corn, Emanuele (2013): *Il principio di precauzione nel diritto penale. Studio sui limiti dell'anticipazione della tutela penale* (Torino, Giappichelli).

Costantini, Federico e Montessoro, Pier Luca (2016): "Il problema della sicurezza tra informatica e diritto: una prospettiva emergente dalle "Smart Cars"", *Informatica e Diritto*, 1, pp. 95-114.

D'Auria, Donato (2017): "Investimento del pedone e prevedibilità in concreto dell'evento dannoso", *Giurisprudenza Italiana*, 2, pp. 469-476.

D'Auria, Donato (2016): "Omicidio stradale: prime osservazioni", *Diritto Penale e Processo*, 4, pp. 432-442.

De Bruine, Jan e Werbrouck, Jarich (2018): "Merging self-driving cars with the law", *Computer Law & Security Review*, 34, pp. 1150-1153.

De Vicente Martínez, Rosario (2008): *Derecho penal de la circulación*, 2a ed. (Barcelona, Bosch).

Delle Cave, Gianluigi (2019): "Il Decreto c.d. Smart Road: sviluppo delle infrastrutture stradali", https://www.altalex.com/documents/news/2018/08/23/il-decreto-cd-smart-road-sviluppo-delle-infrastrutture-stradali, pubblicato il 5.10.2018, ultimo accesso il 19.9.2019.

Di Giovine, Ombretta (2003): *Il contributo della vittima nel delitto colposo* (Torino, Giappichelli).

Donini, Massimo (2004): *Il volto attuale dell'illecito penale. La democrazia penale tra differenziazione e sussidiarietà* (Milano, Giuffrè).

Douma, Frank e Palodichuk, Sarah Aue (2012): "Criminal Liability Issues Created by Autonomous Vehicles", *Santa Clara Law Review*, 52, pp. 1157-1169.

Dovere, Salvatore (2017): "Omicidio e lesioni stradali", in *Il Libro dell'Anno del Diritto 2017* (Roma, Treccani), pp. 152-157.

Duni, Mario (1964): "Limiti all'obbligo di prevedere le imprudenze altrui", *Rivista Giuridica della Circolazione e dei Trasporti*, pp. 317-343.

Feldle, Jochen (2017): "Delicate Decisions: Legally Compliant Emergency Algorithms for Autonomous Cars", in Hilgendorf, Eric e Seidel, Uwe (eds.), *Robotics, Autonomics, and the Law* (Baden-Baden, Nomos), pp. 195-203.

Fiandaca, Giovanni e Musco, Enzo (2014): *Diritto penale. Parte generale*, 7a ed. (Bologna, Zanichelli).

Foot, Philippa (1967): "The problem of abortion and the doctrine of double effect", *Oxford Review*, 5, pp. 5-15.

Forlani, Elisabetta e Planitario, Annamaria (2013): *L'assoluzione dai reati di circolazione stradale nella giurisprudenza* (Santarcangelo di Romagna, Maggioli).

Forti, Gabrio (2006): ""Accesso" alle informazioni sul rischio e responsabilità: una lettura del principio di precauzione", *Criminalia*, pp. 155-225.

Forti, Gabrio (1990): *Colpa ed evento nel diritto penale* (Milano, Giuffrè).

Francis, Leslie P. (2018): "Disability and Automation: The Promise of Cars That Automate Driving Functions", *Journal of Health Care Law & Policy*, 20, pp. 229-252.

Freitas, Pedro Miguel, Andrade, Francisco, Novais, Paulo (2014): "Criminal Liability of Autonomous Agents: From the Unthinkable to the Plausible", in Casanovas, Pompeu, Pagallo, Ugo, Palmirani, Monica, Sartor, Giovanni (eds.), *AI Approaches to the Complexity of Legal Systems (AICOL-IV and AICOL-V International Workshops 2013)* (Berlin-Heidelberg, Springer), pp. 145-156.

Giddens, Anthony (1990): *The Consequences of Modernity* (Cambridge, Polity Press); in traduzione italiana (1994): *Le conseguenze della modernità* (Bologna, Il Mulino).

Giunta, Fausto (2006): "Il diritto penale e le suggestioni del principio di precauzione", *Criminalia*, pp. 227-247.

Giunta, Fausto (1993): *Illiceità e colpevolezza nella responsabilità colposa* (Padova, CEDAM).

Glancy, Dorothy J. (2015): "Autonomous and Automated and Connected Cars Oh My! First Generation Autonomous Cars in the Legal Ecosystem", *Minnesota Journal of Law, Science, and Technology*, 16 (2), pp. 619-691.

Gless, Sabine (2016): ""Mein Auto fuhr zu schnell, nicht ich!" – Strafrechtliche Verantwortung für hochautomatisiertes Fahren", in Gless, Sabine e Seelmann, Kurt (eds.), *Intelligente Agenten und das Recht* (Baden-Baden, Nomos), pp. 225-251.

Gless, Sabine, Silverman, Emily, Weigend, Thomas (2016): "If robots cause harm, who is to blame? Self-driving cars and criminal liability", *New Criminal Law Review*, 19, pp. 412-436.

Gogoll, Jan, Müller, Julian F. (2017): "Autonomous Cars: in Favor of a Mandatory Ethics Setting", *Science and Engineering Ethics*, 23, pp. 681-700.

Goodall, Noah J. (2016): "Away from Trolley Problems and Toward Risk Management", *Applied Artificial Intelligence*, 30 (8), pp. 810-821.

Greenberg, Andy (2015): "Hackers Remotely Kill a Jeep on the Highway – With me in it", *Wired*, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, pubblicato il 21.7.2015, ultimo accesso l'8.3.2019.

Grotto, Marco (2012): *Principio di colpevolezza, rimproverabilità soggettiva e colpa specifica* (Torino, Giappichelli).

Grush, Bern e Niles, John (2019): *The End of Driving* (Amsterdam, Elsevier).

Gurney, Jeffrey K. (2015): "Driving into the Unknown: Examining the Crossroads of Criminal Law and Autonomous Vehicles", *Wake Forest Journal of Law & Policy*, 5 (2), pp. 393.442.

Hallevy, Gabriel (2015): *Liability for Crimes Involving Artificial Intelligence Systems* (Dordrecht, Springer).

Hallevy, Gabriel (2013): *When Robots Kill. Artificial Intelligence under Criminal Law*, (Boston, Northeastern University Press).

Hallevy, Gabriel (2011/2012): "Unmanned Vehicles: Subordination to Criminal Law under the Modern Concept of Criminal Liability", *Journal of Law, Information & Science*, 21 (2), pp. 200-211.

Hallevy, Gabriel (2010): "The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control", *Akron Intellectual Property Journal*, 4, pp. 171-201.

Hanlon, Michelle L.D. (2016): "Self-driving Cars: Autonomous Technology That Needs a Designated Duty Passenger", *Barry Law Review*, 22 (1), pp. 1-26.

Hanna, Katherine L. (2015): "Old Laws, New Tricks: Drunk Driving and Autonomous Vehicles", *Jurimetrics*, 55, pp. 275-289.

Harris, Mark (2014): "FBI warns driverless cars could be used as 'lethal weapons'", *The Guardian*, 16.7.2014.

Hevelke, Alexander e Nida-Rümelin, Julian (2015): "Responsibility for Crashes of Autonomous Vehicles: An Ethical Analysis", *Science and Engineering Ethics*, 21, pp. 619-630.

Hilgendorf, Eric (2017): "Automated Driving and the Law", in Hilgendorf, Eric e Seidel, Uwe (eds.), *Robotics, Autonomics and the Law* (Baden-Baden, Nomos), pp. 171-193.

Hörnle, Tatjana (2009): "Shooting Down a Hijacked Plane´ The German Discussion and Beyond", *Criminal Law and Philosophy*, 3, pp. 111-131.

Kennedy, Caleb (2017): "New Threats to Vehicle Safety: How Cybersecurity Policy Will Shape the Future of Autonomous Vehicles", *Michigan Telecommunications and Technology Law Review*, 23, pp. 343-356.

La Stampa (2019): "Guida autonoma, prime autorizzazioni ai test su strada in Italia: le auto robot a Torino e Parma", 8.5.2019.

Leben, Derek (2017): "A Rawlsian algorithm for autonomous vehicles", *Ethics and Information Technology*, 19, pp. 107-115.

Lee, Chasel (2017): "Grabbing the Wheel Early: Moving Forward on Cybersecurity and Privacy Protections for Driverless Cars", *Federal Communications Law Journal*, 69 (1), pp. 25-52.

Levinson, David (2015): "Climbing Mount Next: The Effects of Autonomous Vehicle on Society", *Minnesota Journal of Law, Science, and Technology*, 16 (2), pp. 787-809.

Lewis, Jeffrey W. (2015): "A Smart Bomb in Every Garage? Driverless Cars and the Future of Terrorist Attacks", *START – National Consortium for the Study of Terrorism and Responses to Terrorism*, https://www.start.umd.edu/news/smart-bomb-every-garage-driverless-cars-and-future-terrorist-attacks, pubblicato il 28.9.2015, ultimo accesso l'8.3.2019.

Lima, Dafni (2018): "Could AI Agents Be Held Criminally Liable? Artificial Intelligence and the Challanges for Criminal Law", *South Carolina Law Review*, 69, pp. 677-696.

LoRicco, Richard (2018): "Autonomous Vehicles: Why We Need Them, But Are Unprepared for Their Arrival", *Quinnipiac Law Review*, 36, pp. 297-325.

Losano, Mario G. (2017): "Il progetto di legge tedesco sull'auto a guida automatizzata", *Diritto dell'Informazione e dell'Informatica*, 1, pp. 1-9.

Luhmann, Niklas (1991): *Soziologie des Risikos* (Berlin, Walter de Gruyter); in traduzione italiana (1996): *Sociologia del rischio* (Milano, Bruno Mondadori).

Magro, Maria Beatrice (2019): "*Robot*, *cyborg* e intelligenze artificiali", in Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo, Papa, Michele (eds.), *Cybercrime* (Milano, UTET-WKI), pp. 1180-1212.

Mantovani, Ferrando (2011): *Diritto penale. Parte speciale*, I, *I delitti contro la persona*, 4a ed. (Padova, CEDAM).

Mantovani, Ferrando (2009): "Il principio di affidamento nel diritto penale", *Rivista Italiana di Diritto e Procedura Penale*, 2, pp. 536-546.

Mantovani, Marco (1997): *Il principio di affidamento nella teoria del reato colposo* (Milano, Giuffrè).

Marchant, Gary E. e Lindor, Rachel A. (2012): "The Coming Collision Between Autonomous Vehicles and the Liability System", *Santa Clara Law Review*, 52, pp. 1321-1340.

Martini, Riccardo (2010): "Incertezza scientifica, rischio e prevenzione. Le declinazioni penalistiche del principio di precauzione", in Bartoli, Roberto (ed.), *Responsabilità penale e rischio nelle attività mediche e d'impresa* (Firenze, Firenze University Press), pp. 579-605.

Matsuo, Takayuki (2017): "The Current Status of Japanese Robotics Law: Focusing on Automated Vehicles", in Hilgendorf, Eric e Seidel, Uwe (eds.), *Robotics, Autonomics and the Law* (Baden-Baden, Nomos), pp. 151-170.

Mattheudakis, Matteo Leonida (2017): "Il guidatore trasgressore semplice, quello collezionista di reati (magari professionista), quello sconsiderato e quello sprovveduto… eventualmente in fuga: anatomia dell'irragionevolezza", *Archivio Penale Web*, 1, pp. 1-52.

Mauer, Markus, Gerdes, J. Christian, Lenz, Barbara, Winner, Hermann (eds.) (2016): *Autonomous Driving. Technical, Legal and Social Aspects* (Dordrecht, Springer).

Mendoza Buergo, Blanca (2001): *El derecho penal en la sociedad del riesgo* (Madrid, Civitas).

Menghini, Antonia (2016): *L'omicidio stradale. Scelte di politica criminale e frammentazione del sistema* (Napoli, Editoriale Scientifica).

Meyer, Gereon e Beiker, Sven (eds.) (2019): *Road Vehicle Automation 5* (Dordrecht, Springer).

Meyer, Gereon e Beiker, Sven (eds.) (2018): *Road Vehicle Automation 4* (Dordrecht, Springer).

Meyer, Gereon e Beiker, Sven (eds.) (2016): *Road Vehicle Automation 3* (Dordrecht, Springer).

Meyer, Gereon e Beiker, Sven (eds.) (2015): *Road Vehicle Automation 2* (Dordrecht, Springer).

Meyer, Gereon e Beiker, Sven (eds.) (2014): *Road Vehicle Automation* (Dordrecht, Springer).

Mezzetti, Enrico (2000): *«Necessitas non habet legem»? Sui confini tra "impossibile" ed "inesigibile" nella struttura dello stato di necessità* (Torino, Giappichelli).

Milder, N. David (2018): "Let's get real about self-driving cars: The transition will take a significant amount of time", *Journal of Urban Regeneration and Renewal*, 11 (3), pp. 223 232.

Militello, Vincenzo (1988): *Rischio e responsabilità penale* (Milano, Giuffrè).

Musacchio, Vincenzo (2007): *Diritto penale della circolazione stradale* (Torino, UTET).

NHTSA (2013): "Preliminary Statement of Policy Concerning Automated Vehicles", https://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf, ultimo accesso il 7.3.2019.

Notaro, Domenico (2016): "I nuovi reati di omicidio stradale e di lesioni personali stradali: norme "manifesto" o specializzazione dello statuto colposo?", *La Legislazione Penale*, 28.7.2016, pp. 1-17.

Nyholm, Sven e Smids, Jilles (2016): "The Ethics of Accident-Algorithms for Self-Driving Cars: an Applied Trolley Problem?", *Ethical Theory and Moral Practice*, 19, pp. 1275-1289.

Pagallo, Ugo (2013): *The Laws of Robots. Crimes, Contracts, and Torts* (Dordrecht, Springer).

Pagallo, Ugo (2011): "Killers, fridges, and slaves: a legal journey in robotics", *AI & Society*, pp. 347-354.

Pagallo, Ugo (2010): "Saggio sui robot e il diritto penale", in Vinciguerra, Sergio e Dassano, Francesco (eds.), *Scritti in memoria di Giuliano Marini* (Napoli, ESI), pp. 595-610.

Palazzo, Francesco (2018): *Corso di diritto penale. Parte generale*, 7a ed. (Torino, Giappichelli).

Palazzo, Francesco e Viganò, Francesco (2018): *Diritto penale. Una conversazione* (Bologna, Il Mulino).

Palodichuk, Sarah Aue (2015): "Driving into the Digital Age: How SDVs Will Change the Law and Its Enforcement", *Minnesota Journal of Law, Science, and Technology*, 16 (2), pp. 827-841.

Pardolesi, Roberto e Davola, Antonio (2017): "In viaggio col robot: verso nuovi orizzonti della r.c. auto («driverless»)?", *Danno e Responsabilità*, pp. 616-629.

Pavich, Giuseppe e Sturlese, Michele Valentino (2018): *Reati stradali* (Milano, Giuffrè).

Pearl, Tracy Hresko (2017): "Fast & Furious: The Misregulation of Driverless Cars", *NYU Annual Survey of American Law*, 73, pp. 19-72.

Piccioni, Fabio (2017): *I reati stradali* (Milano, Giuffrè).

Piergallini, Carlo (2017): "Colpa (diritto penale)", in *Enciclopedia del Diritto. Annali*, X (Milano, Giuffrè), pp. 222-265.

Piergallini, Carlo (2007): "La responsabilità del produttore: una nuova frontiera del diritto penale?", *Diritto Penale e Processo*, 9, pp. 1125-1130.

Piergallini, Carlo (2004): *Danno da prodotto e responsabilità penale. Profili dommatici e politico-criminali* (Milano, Giuffré).

Piergallini, Carlo (1997): "Attività produttive e imputazione per colpa: prove tecniche di «diritto penale del rischio», *Rivista Italiana di Diritto e Procedura Penale*, pp. 1473-1495.

Piergallini, Carlo (1996): "La responsabilità del produttore: avamposto o Sackgasse del diritto penale?", *Rivista Italiana di Diritto e Procedura Penale*, pp. 354-370.

Pollastrelli, Stefano e Acquaroli, Roberto (a cura di) (2017): *Il reato di omicidio stradale* (Milano, Giuffrè).

Pugnetti, Carlo e Schläpfer, Remo (2018): "Customer Preferences and Implicit Tradeoffs in Accident Scenarios for Self-Driving Vehicles Algorithms", *Journal of Risk and Financial Management*, 11 (2), 28, pp. 1-13.

Raue, Martina, D'Ambrosio, Lisa A., Ward, Carley, Lee, Chaiwoo, Jacquillat, Claire, Coughlin, Joseph F. (2019): "The Influence of Feelings While Driving Regular Cars on the Perception and Acceptance of Self-Driving Cars", *Risk Analysis*, 39 (2), pp. 358-374.

Reccia, Eliana (2014): *La criminalità stradale. Alterazione da sostanze alcoliche e principio di colpevolezza* (Torino, Giappichelli).

Riccardi, Giuseppe (2010): *Reati alla guida* (Milano, Giuffrè).

Riondato, Silvio (2017): "Robot: talune implicazioni di diritto penale", in Moro, Paolo e Sarra, Claudio (eds.), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica* (Milano, Franco Angeli), pp. 85-98.

Ruga Riva, Carlo (2006): "Principio di precauzione e diritto penale. Genesi e contenuto della colpa in contesti di incertezza scientifica", in Dolcini, Emilio e Paliero, Carlo Enrico (eds.), *Studi in onore di Giorgio Marinucci*, vol. II, *Teoria della pena. Teoria del reato* (Milano, Giuffrè), pp. 1743-1777.

Russo, Roberta (2010): "Sul principio di affidamento in materia di circolazione stradale", *Cassazione Penale*, 9, pp. 3201-3212.

SAE International (2018): "J3016 Standard", versione originaria del gennaio 2014, ultima revisione del giugno 2018.

Santoni de Sio, Filippo (2017): "Killing by Autonomous Vehicles and the Legal Doctrine of Necessity", *Ethical Theory and Moral Practice*, 20, pp. 411-429.

Scagliarini, Simone (2018): "*Smart roads* e *driverless cars* nella legge di bilancio: opportunità e rischi di un'attività economica «indirizzata e coordinata a fini sociali»", *Quaderni Costituzionali*, 2, pp. 497-500.

Schimelman, Benjamin I. (2016): "How to Train a Criminal: Making Fully Autonomous Vehicles Safe for Humans", *Connecticut Law Review*, 49 (1), pp. 327-354.

Schirò, Dalila Mara (2018): "Omicidio e lesioni personali stradali", in *Dig. Disc. Pen.*, *Agg. X* (Milano, UTET-WKI), pp. 497-515.

Schömig, Nadja, Hargutt, Volker, Neukum, Alexandra, Petermann-Stock, Ina, Othersen, Ina (2015): "The interaction between highly automated driving and the development of drowsiness", *Procedia Manufactoring*, 3, pp. 6652-6659.

Scotti, Silvio Francesco Giuseppe (2016): *La guida in stato di ebbrezza* (Milano, Giuffrè).

Silva Sánchez, Jesús María (2011): *La expansión del derecho penal. Aspectos de la Política criminal en las sociedades postindustriales*, 3a ed. (Montevideo – Buenos Aires, B de F).

State of California Department of Motor Vehicles (2019): "Report of Traffic Collision Involving an Autonomous Vehicle (OL316)", https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/autonomousveh_ol316+ , ultimo accesso il 7.3.2019.

Stilgoe, Jack (2018): "Machine learning, social learning and the governance of self-driving cars", *Social Studies of Science*, 48 (1), pp. 25-56.

Stortoni, Luigi (2004): "Angoscia tecnologica ed esorcismo penale", *Rivista Italiana di Diritto e Procedura Penale*, pp. 71-89.

Suchodolski, Jeanne C. (2018): "Cybersecurity and Autonomous Systems in the Transportation Sector: An Examination of Regulatory and Private Law Approaches with Recommendations for Needed Reforms", *North Carolina Journal of Law & Technology*, 20 (1), pp. 121-197.

Surden, Harry (2014): "Machine Learning and Law", *Washington Law Review*, 89, pp. 87-115.

Surden, Harry e Williams, Mary-Anne (2016): "Technological Opacity, Predictability, and Self-Driving Cars", *Cardozo Law Review*, 38, pp. 121-181.

Taeihagh, Araz e Si Min Lim, Hazel (2019): "Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks", *Transport Reviews*, 39 (1), pp. 103-128.

Teoh, Eric R. e Kidd, David G. (2017): "Rage against the machine? Google's self-driving cars versus human drivers", *Journal of Safety Research*, 63, pp. 57-60.

Thierer, Adam e Hagemann, Ryan (2015): "Removing Roadblocks to Intelligent Vehicles and Driverless Cars", *Wake Forest Journal of Law & Policy*, 5 (2), pp. 339-391.

Tranter, Kieran Mark (2016): "The Challenges of Autonomous Motor Vehicles for Queensland Road and Criminal Laws", *QUT Law Review*, 16 (2), pp. 59-81.

Tronsor, William J. (2018): "The Omnipotent Programmer: an Ethical and Legal Analysis of Autonomous Cars", *Rutgers Journal of Law & Public Policy*, 15 (2), pp. 213-284.

Van Dijk, Alwin e Wolswijk, Hein (eds.) (2014): *Criminal Liability for Serious Traffic Offences* (The Hague, Eleven).

Veneziani, Paolo (2003a): *I delitti contro la vita e l'incolumità individuale. I delitti colposi*, in Marinucci, Giorgio e Dolcini, Emilio (diretto da), *Trattato di diritto penale – parte speciale*, volume 3, tomo 2 (Padova, CEDAM).

Veneziani, Paolo (2003b): *Regole cautelari "proprie" ed "improprie" nella prospettiva delle fattispecie colpose causalmente orientate* (Padova, CEDAM).

Viganò, Francesco (2000): *Stato di necessità e conflitti di doveri. Contributo alla teoria delle cause di giustificazione e delle scusanti* (Milano, Giuffrè).

Waymo (2018): "A Green Light for Waymo's Driverless Testing in California", https://medium.com/waymo/a-green-light-for-waymos-driverless-testing-in-california-a87ec336d657, pubblicato il 30.10.2018, ultimo accesso il 8.3.2019.

Westbrook, Clint W. (2017): "The Google Made Me Do It: The Complexity of Criminal Liability in the Age of Autonomous Vehicles", *Michigan State Law Review*, pp. 97-147.

Westbrook, Holton (2018): "Look Ma, No Hands: Providing Automated Vehicle Regulations and Precedents Inclusive of Disables Individuals", *Texas Tech Administrative Law Journal*, 19, pp. 385-414.

Wing, Christopher (2016): "Better Keep Your Hands on the Wheel in that Autonomous Car: Examining Society's Need to Navigate the Cybersecurity Roadblocks for Intelligent Vehicles", *Hofstra Law Review*, 45, pp. 707-746.

Wolkenstein, Andreas (2018): "What has the Trolley Dilemma ever done for us (and what will it do in the future)? On some recent debates about the ethics of self-driving cars", *Ethics and Information Technology*, 20, 163-173.

Zakharenko, Roman (2016): "Self-driving cars will change cities", *Regional Science and Urban Economics*, 61, pp. 26-37.

Gli algoritmi predittivi per la commisurazione della pena

Los algoritmos predictivos para la determinación de la pena

Predictive Algorithms for Sentencing

Luca D'Agostino
Dottorando di ricerca in diritto e impresa presso l'Università LUISS Guido Carli
ldagostino@luiss.it

Commisurazione della pena | Determinación judicial de la pena | Sentencing

Abstracts

Nell'attuale scenario tecnologico si registra una tendenza crescente alla digitalizzazione dell'amministrazione della giustizia e alla sostituzione del lavoro dell'*homo juridicus* con il *software*. Ciò che potrebbe essere considerato un fattore di semplificazione e modernizzazione, fa sorgere innumerevoli questioni nel momento in cui a essere "rimpiazzate" siano le attività più sensibili, tra cui la valutazione del giudice sulla specie e sulla quantità di pena da irrogare al caso concreto.
L'obiettivo del presente lavoro è quello di fornire al lettore un quadro ricognitivo dell'*evidence-based sentencing* nel processo penale statunitense, con particolare riguardo alla valutazione algoritmica della pericolosità del reo. Analizzando la questione in chiave comparatistica con l'ordinamento italiano, l'utilizzo di questi strumenti rischia di collidere con le garanzie del giusto processo e di scontrarsi con alcuni principi cardine dell'ordinamento processuale. Ciononostante, l'Autore ritiene che sarebbe auspicabile, entro certi limiti e con il rispetto delle doverose accortezze, l'introduzione di tecniche di valutazione attuariale del rischio ai fini della commisurazione della pena.

En el actual escenario tecnológico se registra una creciente tendencia a la digitación de la administración de justicia y a la sustitución del trabajo de las personas con programas informáticos. Lo que podría en un principio ser considerado como un factor de simplificación y modernización, plantea innumerables cuestiones problemáticas en el momento en el que se trata de reemplazar las actividades más sensibles, tales como la determinación de la pena que efectúa el juez en el caso concreto. El objetivo del presente trabajo es ofrecer una reconstrucción general del evidence-bsaed sentencing en el proceso penal estadounidense, con particular atención a la evaluación algorítmica de la peligrosidad del imputado. Analizando la cuestión a la luz del derecho italiano, la utilización de estos instrumentos pareciera colisionar con la garantía del debido proceso y otros principios cardinales del ordenamiento procesal. No obstante, el autor sostiene que sería positivo, dentro de ciertos límites, la introducción de técnicas de evaluación del riesgo en el contexto de la determinación de la pena.

In the current IT scenario, an increasing tendency towards digitalisation of the judiciary can be observed, as well as the substitution of homo juridicus with softwares. An apparent simplification and modernisation factor poses several questions when it comes to "replacing" sensitive activities, including the judicial evaluation on the kind and quantity of punishment in a single case. This paper aims to provide a comprehensive overview of evidence-based sentencing in the US criminal justice system, focusing on the algorithm evaluation of social dangerousness of

the defendant. Looking at the topic from a comparative perspective, in Italy such tools would jeopardise the fair trial safeguards as well as some crucial principles of criminal procedure. Nevertheless, it can be explored the idea of introducing – within some boundaries and taking precautions – certain actuarial risk evaluation techniques in the sentencing process.

Sommario

1. L'intelligenza artificiale nel processo penale. Rilievi introduttivi.

«*Les juges de la nation ne sont que la bouche qui prononce les paroles de la loi, des êtres inanimés, qui n'en peuvent modérer ni la force ni la rigueur*»[1].

La figura del giudice senz'anima, ideata ai tempi dell'Illuminismo francese prerivoluzionario, potrebbe essere considerata una indesiderabile utopia dalla cultura giuridica moderna. Eppure, nell'attuale scenario tecnologico si registra una tendenza crescente alla digitalizzazione dell'amministrazione della giustizia e alla sostituzione lavoro dell'*homo juridicus* con il *software*[2]. Ciò che potrebbe essere considerato un fattore di semplificazione e modernizzazione, fa sorgere innumerevoli questioni nel momento in cui a essere "rimpiazzate" siano le attività più sensibili, tra cui la valutazione del giudice sulla specie e sulla quantità di pena da irrogare al caso concreto.

Gettando uno sguardo alla prassi giudiziaria americana si rinviene una consolidata esperienza sull'impiego di strumenti attuariali di *risk assessment* per aiutare il giudice ad assumere decisioni nella fase cautelare (*pre-trial decisions*), in quella esecutiva (*parole decisions*), e in quella decisoria (*sentencing*)[3].

Il presente contributo rivolge l'attenzione principalmente a quest'ultima fase, nella quale gli algoritmi predittivi fungono da strumento-guida – facoltativo, ma in alcuni casi obbligatorio – nella deliberazione della sentenza di condanna. La valutazione algoritmica della pericolosità lascia aperti numerosi interrogativi sul rispetto delle garanzie difensive dell'imputato, sulla sindacabilità del risultato finale, sulla falsificabilità scientifica del *software*, sull'attendibilità degli *inputs* e dell'*output,* sul residuo dovere di motivazione in capo al giudice, sugli effetti discriminatori dovuti alle generalizzazioni empiriche e ai fattori di condizionamento sociale ed economico processati dall'algoritmo. Alcuni di questi aspetti sono stati affrontati dalla Corte Suprema del Wisconsin del celebre caso *Loomis*[4], con una sentenza che, pur confermando la legittimità del ricorso a questi strumenti, getta una serie di moniti ai giudici di merito sulle cautele da adottare nel farne uso.

L'obiettivo del presente lavoro è quello di fornire al lettore un quadro ricognitivo dell'*evidence-based sentencing* nel processo penale statunitense, con particolare riguardo alla valutazione algoritmica della pericolosità del reo. Analizzando la questione in chiave comparatistica con l'ordinamento italiano, l'utilizzo di questi strumenti rischia di collidere con le garanzie del giusto processo e di scontrarsi con alcuni principi cardine dell'ordinamento processuale. D'altro canto, però, gli studi di settore dimostrano come la valutazione attuariale del rischio di recidiva del reo sia molto più precisa di quella umana, in quanto riesce a processare una immensa quantità di dati di cui nessun giudice potrebbe ragionevolmente disporre. In particolare, l'utilizzo di strumenti di valutazione c.d. di tipo misto – programmati per dare rilevanza non soltanto alle risultanze statistiche, ma anche all'esame della personalità del reo –potrebbe

[1] Montesquieu (1798), p. 248
[2] Sull'autonomia degli agenti *software* e i connessi profili di responsabilità, Teubner (2018) p. 106; Teubner, (2015)
[3] Di recente, Canzio (2018), p. 4
[4] Wisconsin Supreme Court, S*tate v. Loomis*, case 2015AP157-CR, Judgement July 13th 2016, in *Harvard Law Review*, 2017, vol. 130, 1530 ss.

offrire una utile guida per orientare l'attività del giudice nella commisurazione della pena.

A tal fine, nella parte conclusiva del contributo sarà valutata la possibilità di sostituire il modello, attualmente vigente, della *discrezionalità giudiziaria pura* con quello della *discrezionalità condizionata*, nel quale un ruolo significativo potrà essere attribuito agli algoritmi predittivi e, in generale, ai metodi di valutazione attuariale della capacità a delinquere del reo.

2. Finalità della pena e strumenti statistico-attuariali di prevenzione dei reati nel sistema americano.

Negli ultimi anni gli strumenti algoritmici di valutazione del rischio hanno fatto ingresso in diversi uffici della pubblica amministrazione statunitense. La raccolta e l'elaborazione di *big data* è stata accolta con favore dai governi nazionali nella consapevolezza delle incredibili potenzialità che essi offrono in termini di analisi e controllo sociale[5]. La fiducia riposta in questi strumenti emerge chiaramente da loro utilizzo in diversi settori della giustizia penale, dalla polizia predittiva[6] (*predictive policing*) alla valutazione della pericolosità sociale del reo.

L'applicazione del *machine learning* e delle *smart technologies* per la prevenzione di reati è la riedizione moderna di una consolidata tendenza all'utilizzo di strumenti di valutazione del rischio basati su calcoli statistico-attuariali. Pertanto, prima di rivolgere l'attenzione ai moderni *software* di valutazione di rischio, sembra utile richiamare il fondamento storico-dogmatico alla base dell'utilizzo di questi strumenti.

Secondo alcuni autori[7], il dibattito moderno sulla valutazione algoritmica del rischio-reato presenta delle forti similitudini con quello che si ebbe a proposito della teoria dell'inabilitazione selettiva (*selective incapacitation movement*)[8]. La teoria parte dall'assunto che il sistema di giustizia penale dovrebbe essere conformato per consentire una precisa individuazione delle categorie di soggetti socialmente pericolosi – inclini alla violenza o delinquenti professionali o per tendenza – in modo da poterli neutralizzare tenendoli in prigione per lunghi periodi di tempo: l'eliminazione di tali individui dalla società conduce alla riduzione complessiva del tasso di criminalità[9].

La *prevenzione* del crimine mediante la *previsione* ha accompagnato il sistema di giustizia criminale degli Stati Uniti a partite dagli anni '20. Durante gli anni sessanta e i primi anni settanta, gli studi si sono concentrati principalmente sulla ricerca degli indici di pericolosità che confermassero l'attitudine del soggetto alla commissione di crimini violenti[10]. Pur di fronte alle difficoltà di stabilire in modo oggettivo gli indici rivelatori della pericolosità attuale, i fautori della teoria in commento proponevano, seguendo un approccio di tipo utilitaristico, di punire alcuni individui più severamente sulla base del solo giudizio prognostico positivo di recidiva nel reato[11]. La scarsa affidabilità scientifica del metodo ha contribuito a rendere la teoria dell'inabilitazione selettiva un retaggio del passato; residuano tuttavia alcuni istituiti che sembrano rievocarla. Numerosi Stati hanno introdotto statuti autonomi di disciplina per i criminali seriali, istituito presso le Procure reparti specializzati in procedimenti contro criminali professionali, e imposto ai giudici di tener conto dei precedenti penali, della stabilità lavorativa e di altri dati personali.

[5] In argomento, Kehl *et al.* (2017)

[6] Con questa espressione ci si riferisce, in generale, all'insieme di metodi e tecniche utilizzati dall'Autorità di pubblica sicurezza per prevenire la commissione di reati. Di recente il tema è stato ripreso a proposito dell'utilizzo degli algoritmi predittivi per indicare alle forze dell'ordine in tempo reale, secondo criteri probabilistici, le zone metropolitane da sottoporre a controllo o da presidiare. Cfr. Bennett Moses e Chan J. (2018), p. 806

[7] Kehl *et al.* (2017), p. 5

[8] In argomento, si veda l'articolo a cura della Harvard Law Review Association, *Selective Incapacitation: Reducing Crime Through Predictions of Recidivism*, in *Harvard Law Review*, 1982, 96, 2, 511 ss.

[9] I moderni algoritmi di *risk assessment* sono programmati per esprimere un giudizio di pericolosità individuare elaborando dati relativi a categorie di soggetti distinti per età, stili di vita, composizione familiare, provenienza etc. che possa orientare i giudici nella determinazione della pena da irrogare al caso concreto. Si può notare che le premesse di partenza e l'esito decisorio (pena più severa per un individuo ritenuto socialmente pericoloso per l'appartenenza ad una "categoria") riflettono fedelmente i postulati della teoria dell'inabilitazione selettiva.

[10] Tuttavia, la predizione della pericolosità si rivelò alquanto complessa e i primi tentativi ebbero come risultato un notevole numero di falsi positivi. Cfr. Cohen (1983), p.12.

[11] La teoria si fondava sull'assunto che i criminali professionali o per tendenza – responsabili dei delitti più gravi – possono essere facilmente individuati partendo da alcune caratteristiche note, come la loro storia personale e criminale. Tuttavia, la scelta di punire i criminali non per il fatto già commesso, ma per quello che avrebbero potuto commettere in futuro, si scontrava con la tesi di coloro che, sulla base di evidenze statistiche, dimostravano che i crimini attesi potevano in concreto non essere mai commessi. Cfr. Mathiesen (1998), p. 455

Sebbene considerata una "nota a piè di pagina" 12 nella storia della giustizia penale americana, la teoria in commento viene spesso invocata nel dibattito attuale per esprimere dubbi e perplessità sulla precisione algoritmi predittivi e sull'utilizzo di generalizzazioni empiriche basate sull'appartenenza dell'individuo a un gruppo.

Secondo l'opinione di alcuni studiosi[13], la valutazione su basi statistiche della pericolosità del reo è il prodotto della ricostruzione giuridico-filosofica della dottrina statunitense sugli obiettivi della giustizia criminale. Si deve in particolare alla teoria illuminista della funzione rieducativa della pena (*rehabilitation*) il principio secondo cui andrebbe privilegiato un trattamento sanzionatorio che valorizzi le caratteristiche dell'individuo piuttosto che l'offesa che questi ha arrecato; la previsione di sanzioni edittali predeterminate sarebbe dunque d'ostacolo ad una pena individualizzata.

La discrezionalità giudiziaria nella commisurazione della pena, sebbene funzionale alla rieducazione del condannato, aveva comunque sollevato non poche questioni sul piano dell'eguaglianza di trattamento[14]. Parte autorevole della dottrina[15] invocava a gran voce la riforma del *sentencing* federale al fine di ridurre la discrezionalità giudiziaria; il pensiero scientifico del dopoguerra aveva infatti prodotto indagine empiriche a dimostrazione della c.d. *sentencing disparity*; effetto che veniva imputato appunto alla valutazione eccessivamente libera del giudice penale[16]. Dopo alcuni tentativi di riforma[17], una svolta significativa si ebbe con la pubblicazione del volume «Criminal Sentences: Law without Order», libello con cui il giudice Frenkel[18] criticava il modello allora vigente definendolo «*almost wholly unchecked and sweeping*». Gli ideali riformatori furono abbracciati dal senatore Kennedy che, sostenuto da una larga maggioranza, presentò una proposta di legge che costituì la base del *Sentencing Reform Act* del 1984.

Il provvedimento disponeva l'eliminazione della *rehabilitation* come scopo della sanzione detentiva, l'istituzione di una *sentencing commission*, per l'elaborazione di linee guida[19] per la commisurazione della pena e l'introduzione di un sistema di *appellate sentence review*[20]. Prevedeva inoltre che la pena dovesse essere determinata sulla base dell'oggettiva gravità del fatto e delle caratteristiche personali del reo, incluse l'età, l'educazione, le esperienze lavorative, i legami familiari.

2.1. Evidence Based Sentencing *e il modello attuariale di valutazione del rischio.*

La legge di riforma del 1984 segnò il passaggio dalla concezione riabilitativa a quella retributiva della pena. Si affermò l'idea che le condanne penali dovessero essere commisurate all'entità del fatto e alle conseguenze lesive[21], e ponderate sulla base degli elementi individuati nelle *best practise* diffuse a livello federale.

Questo nuovo modello cadeva tuttavia nell'eccesso opposto: se la discrezionalità accordata per la *rehabilitation* dava luogo a disparità di trattamento, la totale compressione del potere discrezionale del giudice conduceva a risultati contrari alle esigenze di giustizia sostanziale. Ben presto si presentò il problema del sovraffollamento carcerario, che gli esperti riconducevano

[12] Kehl *et al.* (2017), p. 6
[13] Cfr. Starr (2014), p. 809, la quale esprime una posizione fortemente critica sugli algoritmi di valutazione della pericolosità del reo, evidenziando come il loro utilizzo sistematico produca intollerabili effetti discriminatori.
[14] Lasciare una eccessiva discrezionalità in mano ai giudici poteva tuttavia sortire effetti negativi sul piano dell'eguaglianza di trattamento. Nel corso della storia è accaduto infatti che i condannati appartenenti a minoranze sociali (linguistiche, etniche, razziali) hanno subito trattamenti sproporzionati rispetto agli esponenti di classi sociali dominanti o altolocate. Cfr. Kehl *et al.* (2017), p. 6
[15] Alla fine degli anni sessanta la dottrina avanzo alcune proposte per l'introduzione di criteri vincolanti nell'esercizio discrezionale, da parte del giudice, della commisurazione della pena. Sul tema, Davis (1969), p. 196
[16] Sul tema, *funditus*, Cannata, (2002)
[17] Nel 1963 fu elaborato un primo *Model Sentencing Act* che prevedeva l'obbligo per il giudice di indicare gli elementi probatori e il ragionamento seguito nell'irrogare la pena del caso concreto. Dalla metà degli anni '60 in poi si affermò l'idea che la discrezionalità giudiziaria dovesse necessariamente essere vincolata al rispetto di parametri legislativamente imposti.
[18] Frankel (1972). Per un commento, Thompson e Starkman (1974) p. 152. L'opera ebbe un impatto notevole sulla scienza giuridica nell'epoca, dal momento che la posizione critica era espressa da un autorevole giudice di merito, che ben conosceva ed esercitava i poteri discrezionali riconosciutigli dalla legge.
[19] Il giudice non è tuttavia libero di disattendere le *sentencing guidelines*. Si tratta quindi di un sistema di *presumptive guidelines*, vale a dire di linee guida aventi forza di legge.
[20] Cannata (2002)
[21] Kehl *et al.* (2017), p. 6

all'espiazione massiva di pene detentive brevi irrogate all'indomani della riforma sul *sentencing*.

In questa parentesi storica iniziò a diffondersi la convinzione che i giudici dovessero basare la decisione sulla quantità di pena – e, se del caso, quella sulla concessione di benefici premiali o di misure alternative alla detenzione – su evidenze statistiche[22] (*evidence-based practices*). La valutazione attuariale del rischio di recidiva nel reato permette al giudice di assumere determinazioni più consapevoli e di scegliere la misura coercitiva o la quantità di pena più appropriata al caso di specie[23]. L'idea di fondo è che il *decision making* nel processo penale non potrebbe (più) fare a meno del sapere scientifico: «As in medicine, psychology, education, management, and other fields, science now offers empirically-derived practice guidelines for criminal justice, which is part of a gradual trend towards the use of evidence-based practices in law»[24].

Secondo l'opinione prevalente[25], un tale approccio costituirebbe la sintesi perfetta tra il paradigma riabilitativo e quello retributivo. Il giudice sarebbe infatti vincolato a tener conto degli elementi oggettivi del fatto, senza trascurare i fattori relativi alla personalità del reo e la sua attitudine a delinquere.

In origine la valutazione del rischio era effettuata caso per caso dagli psicologi penitenziari, i quali si affidavano alle proprie conoscenze professionali e ai risultati del percorso riabilitativo svolto da condannato. Tale sistema presentava il difetto si esprimere risultati difficilmente misurabili e confrontabili tra loro, oltre ad essere inutilizzabile nelle fasi giudiziarie che precedono l'esecuzione della pena. Nel corso degli anni, la *evidence-based-practise* ha potuto contare sul supporto di strumenti predittivi sempre più sofisticati, che considerano l'interazione tra fattori di rischio statici[26] e dinamici[27]. I *tool* di nuova generazione utilizzano algoritmi di apprendimento automatico (*machine learning*), in grado di ponderare tali fattori processando una quantità immensa di dati. Attualmente, le legislazioni di molti Stati prevedono che le Corti possano – e in molti casi debbano – considerare gli *output* forniti dall'algoritmo prima di assumere una determinata decisione.

Per le determinazioni in ordine all'applicazione delle misure cautelari personali e al rilascio su cauzione lo strumento più utilizzato[28] è il *Public Safety Assessment* (PSA), un *software* che utilizza i dati di quasi 2 milioni di reati, commessi in 300 giurisdizioni degli Stati Uniti, per aiutare i giudici a decidere sulla libertà dell'indagato prima che questi sia rinviato a giudizio[29]. In tempi recenti, gli algoritmi predittivi hanno assunto un ruolo centrale anche nella fase dibattimentale (*trial*), quando viene pronunciata una sentenza di condanna ed è necessario stabilire la specie e la quantità di pena da irrogare al caso concreto. Il primo Stato ad elaborare un proprio strumento di *risk-assessment* da utilizzare nella fase decisoria fu il Virginia nel 1994. Altri Stati preferirono utilizzare i prodotti commerciali allora esistenti, tra cui il *Level of Service Inventory – Revised* (LSI-R), in grado di combinare fattori statici e dinamici e di costruire un modello grafico per la determinazione il rischio di recidiva[30].

Tra i *software* privati più evoluti si annovera COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions)* che processa *in input* variabili riconducibili a cinque diverse categorie: precedenti penali, personalità e stile di vita, attitudini personali, composizione familiare, emarginazione sociale. Nelle giurisdizioni di molti Stati, tra cui Wisconsin, Florida e Michigan, questo *software* viene costantemente utilizzato per supportare i giudici nel *sentencing*. Trattandosi di un prodotto brevettato da una società privata, non è noto il codice sorgente

[22] In argomento, di recente, Kingele (2016), p. 537
[23] Le *evidence-based practise* utilizzano i dati relativi alle condizioni socio-economiche e i risultati di *test* specifici per valutare la pericolosità del condannato e il rischio di recidiva nel reato; l'obiettivo di questi metodi è di ridurre le probabilità che questi ritorni a delinquere. I criminali vengono generalmente raggruppati in base al punteggio in tre fasce di rischio (alto, medio e basso).
[24] Così, Redding (2009), p. 2
[25] Faigman e Monahan (2005), p. 642
[26] I *fattori di rischio statici* comprendono, ad esempio, i precedenti penali, l'età del soggetto al primo arresto e il sesso. Pur essendo sintomatici della pericolosità sociale del reo, questi fattori non sono tenuti in considerazione ai fini del trattamento in quanto immodificabili. Tuttavia, sono spesso utilizzati insieme ai fattori dinamici per valutare il rischio di recidiva nel reato. I primi metodi di valutazione attuariale del rischio, sviluppati negli anni settanta, consideravano principalmente i fattori statici; ciò rendeva impossibile valutare i progressi positivi del percorso di riabilitazione, dando luogo a possibili effetti discriminatori per i soggetti che presentavano indici di rischio-base molto elevati.
[27] I *fattori di rischio dinamici* – meglio noti come *necessità criminogene* – sono variabili nel tempo e includono l'età attuale, lo *status* occupazionale, l'uso di sostanze alcoliche o stupefacenti. Tali fattori vengono spesso considerati per individuare il trattamento più idoneo a diminuire la probabilità di recidiva.
[28] Il PSA è stato adottato in 29 giurisdizioni americane, tra cui tutti i distretti giudiziari di Arizona, Kentucky e New Jersey. Per informazioni di dettaglio, si veda il sito https://www.psapretrial.org
[29] Il *software* determina il rischio sulla base dei fattori statici, classificando il profilo dell'indagato persona come persona a basso rischio, che può quindi essere rilasciata, ovvero ad alto rischio, che dovrebbe essere trattenuta.
[30] Starr (2014), p. 809

dell'algoritmo, né il peso che viene attribuito a ciascuna variabile. Nel prosieguo della trattazione avremo modo di esaminare le numerose questioni che ciò solleva sul piano giuridico e le prime posizioni espresse in merito dalla giurisprudenza statunitense.

2.2. Presentencing Investigation Reports *e la deliberazione della sentenza di condanna.*

Il procedimento seguito dalle Corti distrettuali per la determinazione della pena si caratterizza per l'esistenza di una fase di istruttoria preliminare, finalizzata ad ottenere un profilo socio-criminologico dell'imputato. Quando, a chiusura del dibattimento (*trial*), viene pronunciata sentenza di condanna, il giudice attende il deposito del *presentencing investigation report* (PSI) nel quale sono inseriti elementi utili a determinare la specie e la quantità di pena. Della redazione del rapporto viene solitamente incaricato un ausiliario con esperienza nel settore socio-assistenziale o con competenze nelle scienze psicologiche o criminologiche. La relazione include informazioni di dettaglio sulla biografia, sui precedenti penali dell'imputato e sui risultati delle interviste a familiari, *ex* datori di lavoro, amici e conviventi.

La legge non pone restrizioni sugli elementi che possono confluire nel *report*. L'istruttoria *de qua* è sottratta ai principi generali del modello accusatorio[31], per cui il giudice è libero di prendere in considerazione tutti gli elementi che ritenga utili, anche se non oggetto di contraddittorio tra le parti. Una volta depositato nella cancelleria della Corte, la relazione è resa disponibile alla difesa; può tuttavia essere limitato l'accesso ad alcune parti del documento o ad alcune informazioni classificate come confidenziali. La limitazione all'accesso garantisce gli individui sentiti nel corso dell'istruttoria da possibili ritorsioni da parte del condannato, incentivandoli in tal modo a cooperare con la giustizia.

Depositato il PSI, il processo si conclude con l'udienza finale c.d. di condanna, all'esito della quale il giudice assumerà – seguendo il suo libero convincimento – la decisione sulla pena da irrogare al condannato, basandosi su tutte le prove disponibili, ivi comprese quelle che le parti presentano alla medesima udienza.

La fase istruttoria che precede l'irrogazione della pena è la fase del processo in cui la valutazione algoritmica del rischio ha assunto maggior rilievo. Guardando alla legislazione più recente, alcuni studiosi[32] hanno rilevato una crescente tendenza degli Stati ad imporre ai giudici vincoli sempre più stringenti nel *sentencing*.

In alcune giurisdizioni l'utilizzo di strumenti di *risk assessment* è imposto dalla legge. In Arizona, ad esempio, si richiede specificamente che i PSI contengano informazioni specifiche *«related to criminogenic risk and needs as documented by the standardized risk assessment and other file and collateral information»*[33]. Parimenti, in Oklahoma è imposto l'utilizzo di *«assessment and evaluation instrument designed to predict risk of recidivism to determine eligibility for any community punishment»*[34]. Una legge dello Stato dell'Ohio aveva affidato al Dipartimento della giustizia penitenziaria il compito di individuare un affidabile strumento di valutazione del rischio che potesse essere utilizzato per diverse finalità, tra cui la commisurazione della pena[35]. È stato così creato l'Ohio Risk Assessment System (ORAS), un *software* di valutazione del rischio messo a punto da un *team* di esperti e di accademici dell'Università di Cincinnati.[36]

Altri Stati[37] hanno adottato un approccio più cauto, promuovendo buone pratiche di EBS, senza però imporre l'uso di strumenti predittivi. In un recente caso la Corte Suprema dell'Indiana ha invitato i giudici di merito a fare uso di tali strumenti, sottolineando con enfasi che la letteratura scientifica *«has demonstrated for decades that objective actuarial risk/needs instruments*

[31] L'eccezione si giustifica per le peculiarità di questa fase processuale. L'istruttoria sulla personalità dell'imputato non potrebbe certamente essere condotta prima o durante il dibattimento, per evidenti ragioni di estraneità rispetto al *thema probandum* e di rispetto del principio di terzietà e di imparzialità del giudice.
[32] Kehl *et al.* (2017), p. 15 cui si rinvia per approfondimenti circa le legislazioni dei singoli Stati sull'utilizzo di strumenti di valutazione algoritmica e attuariale del rischio. Cfr. https://epic.org/algorithmic-transparency/crim-justice
[33] Ariziona Justice Administration Code, § 6–201.01(J)(3).
[34] Kehl *et al.* (2017), p. 15
[35] Ohio Revised Code, § 5120.114(A), (1-3).
[36] Sulla creazione di ORAS, di recente Singh *et al.* (2018)
[37] Tra cui Louisiana, Idaho, Indiana, Maryland, Alaska.

more accurately predict risk and identify criminogenic needs than the clinical judgment of officers»[38].

Trattandosi di una materia regolata in modo tutt'altro che omogeneo nelle diverse giurisdizioni, l'American Law Institute ha proposto una riforma della parte del *Model Penal Code*[39] dedicata al *sentencing*, avente ad oggetto proprio gli strumenti di valutazione del rischio. Si prevede che i giudici debbano considerare i risultati della misurazione del rischio prima di emettere la sentenza dal momento che le valutazioni statistico-attuariali «*derived from objective criteria, that have been found superior to clinical predictions built on the professional training, experience, and judgment of the persons making predictions In short, recidivism risk prediction is inevitably part of sentencing, and rather than being guided by judges' unreliable 'clinical' assessments of offenders, it should be guided by the best available scientific research*»[40]. Nelle note integrative alla proposta si rimarca però la necessità di garantire la precisione e l'affidabilità di tali strumenti, e di far sì che vengano utilizzati in modo trasparente e nel rispetto del diritto di difesa del condannato[41].

In tempi recenti, le più alte istituzioni del sistema giudiziario statunitense, tra cui l'Adunanza dei *Chief Justices* e la Conferenza degli *State Court Administrators*, hanno lanciato alcune iniziative per lo sviluppo di buone pratiche per l'*evidence based sentencing.*[42] Si registrano comunque anche voci di segno contrario. Il *Department of Justice* ha espresso una posizione piuttosto scettica nei confronti degli algoritmi predittivi, mettendo in guardia i legislatori nazionali sui possibili effetti discriminatori del loro utilizzo su individui provenienti da classi sociali disagiate[43].

2.3. *Valutazione del rischio e interferenza con le finalità della pena.*

Una prima questione affrontata dalla dottrina americana riguarda il rapporto tra il rischio di recidiva e la commisurazione della pena. La circostanza che gli algoritmi predittivi fossero già utilizzati con successo in altre fasi del processo penale aiuta a comprendere perché i legislatori nazionali, o talvolta gli stessi giudici, abbiano avvertito l'esigenza di farne uso anche nel *sentencing*.

Nondimeno, l'assimilazione dei due contesti decisionali dovrebbe seguire una certa cautela. Nella maggioranza dei casi, i *software* sono stati programmati per supportare le decisioni di *pre-trial release*; il giudizio prognostico effettuato in questa fase ha lo scopo di prevedere se il convenuto, nelle more della celebrazione del processo, si asterrà o meno dal commettere altri delitti. Il giudice si troverà di fronte un *aut-aut*: qualora ritenga l'imputato ad alto rischio di recidiva, opterà per la custodia cautelare; in caso contrario, non sussistendo altre esigenze cautelari, potrà disporne la liberazione.

Quando viene pronunciata una sentenza di condanna, l'*iter* decisionale risulta ben più articolato e complesso, dovendo il giudice stabilire non solo quale pena irrogare, ma anche in quale misura. Le determinazioni sul *quantum puniatur* sono condizionate dalle diverse teorie sulle funzioni della pena (retributiva, rieducativa, preventiva).

Alcuni autori[44] ritengono che vi sia un legame di proporzionalità diretta tra la pericolosità sociale e la rieducazione del condannato, tale per cui gli individui a basso rischio di recidiva dovrebbero sempre essere considerati buoni candidati per la *rehabilitation*. L'attitudine a delinquere di alcuni condannati farebbe invece arretrare le esigenze di risocializzazione di fronte alla necessità di una loro inabilitazione a lungo termine (o addirittura permanente) al fine di proteggere l'incolumità pubblica. Questa tesi, che richiama l'idea positivista dell'efficacia

[38] Malenchik v. State, sentenza del 09 giugno 2010, repertorio dello Stato dell'indiana n. 928 N.E.2d 564, § 7
[39] Model Penal Code, Sentencing, Tentative Draft No. 3 (April 24, 2014), presentato al Consiglio dell'American Law Institute, https://ali.org. Il paragrafo § 6B.09 richiede l'uso di «*actuarial instruments or processes, supported by current and ongoing recidivism research, that will estimate the relative risks that individual offenders pose to public safety […] when these instruments or processes prove sufficiently reliable*». Il Model Penal Code è un codice elaborato dell'American Law Insistitute, pubblicato per la prima volta nel 1962 e sottoposto a revisione e aggiornamento periodici. Si tratta di un testo redatto in articoli, la cui stesura è affidata a un gruppo di esperti, che funga da guida per i legislatori nazionali per riformare e uniformare le legislazioni penali interne nelle materie di competenza domestica.
[40] In questi termini la sezione § 6B.09, 53-55 (Tentative Draft No. 2, 2011)
[41] In argomento, Starr (2014), p. 815
[42] Tra gli obiettivi del progetto figura la riduzione del tasso di pene detentive da scontare in carcere attraverso una accurata profilazione dei criminali a basso rischio di recidiva.
[43] Kehl *et al.* (2017), p. 16
[44] Per gli opportuni riferimenti si rinvia a Kehl *et al.* (2017), p. 13; Hartcourt (2005), p. 32

special-preventiva della pena[45], lascia adito a molti dubbi. Non vi è infatti alcuna fondata evidenza scientifica che confermi gli effetti positivi della lunga incarcerazione sulla probabilità di recidiva dell'individuo.

Detto altrimenti, non necessariamente all'aumentare della pena detentiva diminuirà la probabilità che il condannato ritorni a commettere reati. Ricevuti i risultati della valutazione algoritmica del rischio, è verosimile che la decisione finale dipenda dalle convinzioni personali del giudice sulle finalità della pena.

Sarebbe pertanto opportuno che questi strumenti fossero utilizzati a supporto delle sentenze di condanna in modo critico e costruttivo. Il giudicante dovrebbe anzitutto considerare lo scopo della sanzione penale, per valutare l'effettiva utilità di questi strumenti e la reale incidenza del punteggio di rischio (*risk score*) sulla qualità e quantità di pena da irrogare al caso concreto.

3. Il caso *Loomis vs State of Wisconsin*.

La celebre decisione della Suprema Corte nel caso *Loomis v. State of Wisconsin*[46]ha riacceso il dibattito sulle tecniche di valutazione statistico-attuariale del rischio, con particolare riguardo alla legittimità dell'impiego di algoritmi predittivi coperti da diritti di proprietà industriale. Trattandosi del *leading case* più rilevante in materia, ci pare opportuno ripercorrere, sia pur con sinteticità, la vicenda e le questioni affrontate dalla Corte.

Il Sig. Loomis, tratto in giudizio con l'accusa di aver partecipato ad una sparatoria tra autoveicoli, viene condannato, a seguito della riqualificazione del fatto, per aver volontariamente evitato il posto di blocco degli agenti di polizia e per essersi impossessato di una autovettura senza il consenso del proprietario[47]. Nella fase di istruttoria precedente alla deliberazione della sentenza di condanna, l'ufficiale del Dipartimento di polizia penitenziaria produce una relazione PSI, contenente i risultati della valutazione del rischio effettuata con COMPAS, basata sulle risposte fornite dal condannato nel corso di un'intervista e sul profilo criminologico di quest'ultimo. All'udienza finale la Corte – esaminati gli esiti della valutazione del rischio, che evidenziavano una particolare proclività a delinquere del soggetto[48] – determina la pena in sei anni di reclusione e successivi cinque anni di sorveglianza speciale. Pochi giorni dopo, Loomis propone al giudice del dibattimento una istanza di liberazione (*motion for post-conviction relief*), deducendo che il richiamo ai risultati generati dall'algoritmo aveva leso il proprio diritto di difesa. La difesa lamentava, in particolare, l'impossibilità di esaminare la metodologia di calcolo usata da COMPAS, coperta da segreto di fabbrica (*trade secret*) e la acritica estensione nei suoi confronti di statistiche generali che davano luogo, rispettivamente, alla violazione del diritto ad essere basato sulle base di prove oggettive (*right to be sentenced on accurate information*) e del diritto alla individualizzazione del trattamento (*right to an individualized sentence*). Viene inoltre contestata la legittimità costituzionale della condanna, basata su valutazioni che tengono conto, in modo evidentemente sfavorevole all'imputato, del genere (maschile) di appartenenza, dato che secondo la difesa dovrebbe essere ritenuto del tutto neutrale.

L'istanza di liberazione viene respinta dalla *trial court* con provvedimento impugnato dinanzi alla *Court of Appeals,* la quale decide di riferire il caso alla Wisconsin Supreme Court. I giudici di legittimità, all'unanimità, rigettano il ricorso, affermando che l'utilizzo di COMPAS nel *sentencing* non lede i diritti processuali e le garanzie di difesa dell'imputato, purché i giudici lo utilizzino come mero strumento di supporto nella commisurazione della pena

[45] Nel pensiero positivista la pena è priva di qualsiasi finalità di retribuzione. Essa dovrebbe essere unicamente considerata come un mezzo per la difesa sociale: tale sanzione non può dunque avere durata prestabilita, in proporzione alla gravità del fatto commesso, dovendo piuttosto essere indeterminata in quanto vincolata al tempo necessario a eliminare la condizione di pericolosità nel soggetto e riadattarlo alla vita libera nella società.

[46] Wisconsin Supreme Court, S*tate v. Loomis*, case 2015AP157-CR, cit.

[47] La narrazione del fatto e le argomentazioni delle parti sono riprodotte nel commento alla sentenza sulla *Harvard Law Review*, 2017, vol. 130, 1531.

[48] In base ai dati processati da COMPAS l'imputato sarebbe un soggetto altamente pericoloso, avendo riportato un punteggio molto nelle tre forme di recidiva misurate dal *software*: recidiva generica, recidiva a carattere violento, e recidiva immediata (precedente alla condanna). L'interfaccia di COMPAS permette di ottenere i risultati della valutazione algoritmica del rischio in forma di diagramma a barre, con scalarità da 1 a 10. Che la valutazione espressa dall'algoritmo abbia influito in modo decisivo sul giudizio della Corte è confermato dalle parole che il giudice Scott Horne ha rivolto all'imputato nel corso dell'udienza finale: «*The risk assessment tools that have been utilized suggest that you're extremely high risk to reoffend*» (Wisconsin Supreme Court, S*tate v. Loomis*, cit., § 19).

e non considerino l'indice di pericolosità del reo un fattore *ex se* aggravante o attenuante[49]. Contro la sentenza l'imputato ha presentato un *petition* alla Suprema Corte degli Stati Uniti per ottenere un *writ of certiorari*, ravvisando una violazione del quattordicesimo emendamento alla Costituzione degli Stati Uniti[50]. A seguito dello scambio di memorie, acquisito il parere del governo federale e del *General Solicitor*, la richiesta è stata definitivamente respinta con ordinanza della Corte[51].

3.1. *Le argomentazioni della Corte*

Dopo aver ripercorso lo svolgimento del processo e le prospettazioni delle parti, l'estensore ripercorre i singoli motivi di ricorso, esplicitando le ragioni per cui il Collegio ha ritenuto di doverli disattendere.

Con riferimento al primo motivo, con cui si lamenta la violazione del *right to a fair trial* per effetto dell'impossibilità di sindacare le determinazioni dell'algoritmo e la precisione dello strumento di calcolo, la Corte ritiene non risolutiva la circostanza che si tratti di un *software* privato, protetto dai diritti di proprietà industriale. Pur essendo del tutto ignote le modalità con cui il *tool* procede alla ponderazione dei vari fattori di *input*, rimane il fatto che le informazioni più rilevanti processate dall'algoritmo sono state fornite dall'imputato nel corso dell'interrogatorio oppure ricavate dai suoi precedenti penali[52]. Ciò destituisce di fondamento la prospettazione relativa alla violazione del *right to be sentenced on accurate information*, ben potendo la difesa verificare la correttezza degli *input* e sollevare questioni sulla irragionevolezza dell'*output* in relazione ai dati in ingresso processati dalla macchina.

Le doglianze in merito alla violazione del *right to an individualized sentence* sono, ad avviso della Corte, parimenti infondate. Per argomentare l'estensore ricorre ad una *distinctio* tra il caso in cui il punteggio ottenuto a seguito della valutazione algoritmica del rischio sia il fattore determinante nella commisurazione della pena (*the only factor or the determinative factor*), e quello in cui l'*assessment* sia soltanto un segmento del patrimonio informativo a disposizione del giudice[53]. Nel primo caso, di scuola, è indiscutibile che l'applicazione di dati basati su generalizzazioni empiriche, legate in particolare all'appartenenza del soggetto a un gruppo di individui, giungerebbe a violare apertamente il diritto ad un trattamento individualizzato, riflesso del generale principio del giusto processo. Altrettanto non potrebbe dirsi nella seconda ipotesi, conforme alla realtà dell'ordinamento processuale vigente. L'individualizzazione del trattamento viene garantita dall'esistenza di un potere discrezionale nelle mani del magistrato e dal principio secondo cui le prove dovranno essere valutate con prudente apprezzamento. Così, anche gli esiti delle indagini statistiche sulla pericolosità del reo, indipendentemente dalle tecniche o dal metodo scientifico utilizzati, dovranno essere sottoposti ad un previo

[49] «*It is very important to remember that risk scores are not intended to determine the severity of the sentence or whether an offender is incarcerated. Risk and need assessment information should be used in the sentencing decision to inform public safety considerations related to offender risk reduction and management […] It should not be used as an aggravating or mitigating factor in determining the severity of an offender's sanction. Additionally, we set forth the corollary limitation that risk scores may not be used as the determinative factor in deciding whether the offender can be supervised safely and effectively in the community*» (Wisconsin Supreme Court, S*tate v. Loomis*, § 93).

[50] La Section 1 riconosce il diritto ad un equo processo in questi termini: «*No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws*».

[51] Lo si apprende dal sito istituzionale della Corte Suprema federale nella sezione «Case documents», Order 26th June 2017, No. 16-6387, https://www.supremecourt.gov

[52] Di seguito i passaggi più significativi dell'*iter* argomentativo: «*Loomis contends that because a COMPAS risk assessment is attached to the PSI, a defendant is denied full access to information in the PSI and therefore cannot ensure that he is being sentenced based on accurate information […] Additionally, Loomis contends that unless he can review how the factors are weighed and how risk scores are determined, the accuracy of the COMPAS assessment cannot be verified. Loomis is correct that the risk scores do not explain how the COMPAS program uses information to calculate the risk scores. However, Northpointe's 2015 Practitioner's Guide to COMPAS explains that the risk scores are based largely on static information (criminal history), with limited use of some dynamic variables (i.e. criminal associates, substance abuse). Thus, to the extent that Loomis's risk assessment is based upon his answers to questions and publicly available data about his criminal history, Loomis had the opportunity to verify that the questions and answers listed on the COMPAS report were accurate*» (Wisconsin Supreme Court, S*tate v. Loomis*, § 46 ss.).

[53] La Corte sottolinea in particolare che: «*If a COMPAS risk assessment were the determinative factor considered at sentencing this would raise due process challenges regarding whether a defendant received an individualized sentence. As the defense expert testified at the post-conviction motion hearing, COMPAS is designed to assess group data. He explained that COMPAS can be analogized to insurance actuarial risk assessments, which identify risk among groups of drivers and allocate resources accordingly.* […] *Ultimately, we disagree with Loomis because consideration of a COMPAS risk assessment at sentencing along with other supporting factors is helpful in providing the sentencing court with as much information as possible in order to arrive at an individualized sentence. COMPAS has the potential to provide sentencing courts with more complete information to address this enhanced need*» (Wisconsin Supreme Court, S*tate v. Loomis*, § 67 ss.).

vaglio di compatibilità con le informazioni a disposizione del giudice.

Venendo all'ultimo motivo di ricorso in punto di inutilizzabilità dei risultati del *risk assessment*, il ricorrente lamenta la illegittimità costituzionale di una valutazione algoritmica che tiene conto del genere di appartenenza come fattore di innalzamento del punteggio base di rischio. A tal riguardo viene invocato un noto precedente con cui Corte Suprema federale del 1976 aveva ritenuto che la disparità di trattamento tra uomini e donne, ancorché basata su dati empirici, non fa venire meno la violazione della *equal protection clause* di cui al quattordicesimo emendamento[54]. Il Collegio ritiene tuttavia di non poter aderire alla tesi difensiva poichè «*if the inclusion of gender promotes accuracy, it serves the interests of institutions and defendants, rather than a discriminatory purpose*»[55]. Inoltre, nel caso in esame la censura non potrebbe dirsi rilevante, non essendo stato allegato, né provato, che l'appartenenza al genere maschile abbia condizionato la decisione del giudice sulla pena da irrogare. Dalla lettura della sentenza di primo grado non si evince infatti alcun passaggio logico giuridico (*explanation of the rationale*) che consenta di affermare che il fattore sessuale abbia inciso sulla valutazione attuale della pericolosità dell'imputato.

Terminato l'esame dei singoli motivi di ricorso, il percorso argomentativo si conclude con un inaspettato *caveat* sull'utilizzo degli algoritmi predittivi nel processo penale. L'estensore ricorda che molti dei *software* utilizzati per la valutazione del rischio sono di natura proprietaria e non permettono alcuna «*disclosure of specific information about the weights of the factors or how risk scores are calculated*»[56]. Il risultato della valutazione potrebbe inoltre essere falsato dalla classificazione di individui appartenenti a minoranze sociali e dall'assenza di studi scientifici che dimostrino la specifica applicabilità del campione di dati alla popolazione locale[57]. I giudici di merito dovrebbero quindi procedere con una certa cautela nel far uso di questi strumenti, specialmente quando i risultati della valutazione confluiscano nel PSI e siano utilizzati ai fini della determinazione della pena[58].

3.2. *Verso una razionalizzazione della discriminazione?*

Pur avendo esaminato a fondo le problematiche legate all'utilizzo di strumenti predittivi, la sentenza *Loomis* lascia insolute numerose questioni.

Pronunciandosi sul terzo motivo di ricorso, la Corte sembra accontentarsi della circostanza che i giudici di merito, almeno formalmente, non abbiano tenuto conto degli effetti discriminatori discendenti dall'appartenenza dell'individuo a un gruppo, nella specie a quello dei *male sex offenders*. Così facendo sottovaluta però la reale portata del problema.

Per quanto il punteggio di rischio sia determinato processando i dati raccolti *hic et nunc*, rimane il fatto che il soggetto viene inquadrato in un profilo socio-criminale basato sul tasso di recidiva *in consimili casu*. L'obiezione principale mossa dagli studiosi americani riguarda l'inclusione, tra le variabili rilevanti ai fini della determinazione del livello di rischio, di fattori demografici, socioeconomici, familiari, che contribuiscono a caratterizzare come individui più pericolosi quelli appartenenti a determinate minoranze o classi sociali[59]. Gli algoritmi predittivi utilizzano *Big Data* sui precedenti penali degli ultimi decenni per catalogare i cri-

[54] US Supreme Court, *Craig v. Boren*, 1976, 429 US, 190, disponibile su https://www.supremecourt.gov nella sezione "*case law*". Nel celebre caso la Corte Suprema aveva dichiarato incostituzionale per violazione del quattordicesimo Emendamento una legge dell'Oklahoma che vietava la vendita di sostanze alcoliche ai minori di anni 21 di genere maschile, esentando dal divieto le donne che avessero compiuto gli anni 18.

[55] Wisconsin Supreme Court, S*tate v. Loomis*, cit., § 83

[56] Wisconsin Supreme Court, S*tate v. Loomis*, cit., § 66

[57] Nella *concurring opinion* Justice Abrahamson evidenzia a chiare lettere la necessità che i giudici di merito seguano un processo logico-argomentativo per saggiare l'attendibilità dello strumento predittivo utilizzato. «*I write separately to make two points: First, I conclude that in considering COMPAS (or other risk assessment tools) in sentencing, a circuit court must set forth on the record a meaningful process of reasoning addressing the relevance, strengths, and weaknesses of the risk assessment tool. Second, this court's lack of understanding of COMPAS was a significant problem in the instant case. At oral argument, the court repeatedly questioned both the State's and defendant's counsel about how COMPAS works. Few answers were available*» (Wisconsin Supreme Court, S*tate v. Loomis*, cit., § 133).

[58] L'estensore ricorda che COMPAS, pur essendo un algoritmo molto evoluto, è stato progettato per supportare le decisioni giudiziarie nella fase di esecuzione della pena (*for correctional purposes*), ma non anche quelle in ordine alla commisurazione della pena (*sentencing*).

[59] COMPAS, ad esempio, tiene conto delle condanne penali riportate dai genitori dell'imputato, dell'uso di sostanze tossiche o stupefacenti, o di eventuali reati di cui i componenti del nucleo familiare siano stati vittime in passato. LSI-R considera tra i fattori rilevanti anche l'intervento dei servizi sociali, i voti conseguiti alle scuole superiori, le possibilità di trovare un lavoro con un buono stipendio, il tasso di criminalità del quartiere in cui il soggetto vive o è cresciuto. Sul punto, Starr (2014), p. 813

minali in gruppi e sottoinsiemi, ai quali è attribuito un valore di rischio. I dati forniti in *input* descrivono il profilo del criminale e concorrono a determinare la sommatoria dei punteggi (positivi o negativi) riferiti alle singole categorie di appartenenza, ma l'*output* risulta – per così dire – contaminato dal *trend* storico al trattamento deteriore e al pregiudizio nei confronti di alcune figure di criminali. Invero, per garantire una maggiore affidabilità, i *software* attingono da un database molto esteso che ricomprende anche quei periodi storici in cui, per comune esperienza, vi era tendenza alla discriminazione etnica e alla soggettivizzazione della pena. Le indagini statistiche condotte negli ultimi anni dimostrano come le variabili di carattere socio-economico, relative alla provenienza etnica[60] o al grado di scolarizzazione[61] siano spesso un fattore determinante nella misurazione del rischio di recidiva. Non essendo noto il peso che, nella valutazione complessiva, gli algoritmi predittivi attribuiscono ai fattori *de quibus*, potrebbe ben darsi che un soggetto appartenente ad una categoria "a rischio" sia ritenuto più pericoloso sulla base di mere generalizzazioni (*group-based generalizations*). Essendo evidente l'effetto discriminatorio prodotto dalle variabili socioeconomiche, alcuni autori suggeriscono di espungerle dai parametri di *risk assessment,* limitando l'analisi ai soli precedenti penali del reo, all'età al primo arresto, e alle caratteristiche del crimine commesso[62].

3.3. Fairness, transparency *e sindacabilità* dell'output.

La *concurring opinion* del giudice Abrahamson evidenzia a chiare lettere la scarsa trasparenza del funzionamento degli algoritmi predittivi[63]. La preoccupazione maggiore riguarda l'impossibilità per i giudici di conoscere con precisione quali siano i fattori di *input* considerati dal *software*, e come tali fattori siano ponderati tra loro.

L'imbarazzo di fronte alla "impenetrabilità" della macchina è acuito dall'utilizzo del linguaggio di programmazione: quand'anche il codice sorgente fosse noto, il giudice non potrebbe sapere come gli assunti del ragionamento umano sono stati tradotti in codice dagli sviluppatori, né potrebbe da sé verificare la correttezza di tali assunti. Rimane inoltre il problema della compatibilità dell'uso di strumenti progettati per decisioni *pre-trial* al *sentencing*. Quando uno strumento viene sviluppato per un contesto, come la valutazione del rischio per la concessione di misure alternative alla detenzione, non è detto che possa essere automaticamente riadattato per la commisurazione della pena. L'aura oscura che avvolge gli indici rivelatori della pericolosità (e il peso ad essi attribuito) limita sensibilmente il diritto di difesa dell'imputato che non è messo in condizione di sindacare l'*output* della valutazione e di verificarne la correttezza (anche solo) formale.

A ben vedere, in un ordinamento processuale regolato dal principio del contraddittorio nella formazione della prova si dovrebbe assicurare una *discovery* completa su tutti gli elementi di prova utilizzati contro l'imputato. Desta dunque stupore che le argomentazioni del giudice Abrahamson abbiano trovato spazio soltanto in una opinione separata e non discordante rispetto alla decisione assunta dal collegio[64].

Tanto premesso sull'esperienza statunitense, rivolgiamo ora lo sguardo al sistema italiano per esaminare se gli strumenti e le tecniche di *risk assessment* per la commisurazione della pena possano trovare impiego all'interno del processo penale.

[60] Secondo le statistiche generali, negli Stati Uniti un uomo di colore dovrebbe essere considerato cinquanta volte più pericoloso rispetto a una donna bianca. Tra gli individui a più alto rischio di recidiva figurano in particolare i giovani di colore, atteso che attualmente uno su nove, di età ricompresa tra i 20 e i 35 anni, è sottoposto a misura cautelare o sconta una pena detentiva di tipo custodiale. Secondo una analisi condotta nel 2003 dal Dipartimento della Giustizia federale un terzo degli uomini di colore è finito dietro le sbarre almeno una volta nella vita. Per approfondimenti, Starr (2014), p. 837; Bonczar (2003)

[61] In base ad un recente studio, gli individui che non hanno portato a termine gli studi superiori sarebbero 47 volte più pericolosi rispetto a coloro che hanno conseguito il diploma. Sum *et al.* (2009)

[62] Cfr. Starr (2014), p. 850; Kehl *et al.* (2017), p. 25

[63] Wisconsin Supreme Court, *State v. Loomis*, cit., § 130

[64] Il requisito della trasparenza è di fondamentale importanza per ipotizzare un utilizzo degli algoritmi predittivi nel processo penale italiano. V. *Amplius,* § 5

4. Uno sguardo al sistema penale italiano. Quali limiti all'introduzione di una valutazione algoritmica della pericolosità del reo?

Nel nostro sistema penale, la commisurazione della pena è una attività demandata alla valutazione discrezionale del giudice. L'art. 133 c.p. prevede che il giudice debba tener conto sia della gravità del reato (comma 1), sia della capacità a delinquere del colpevole (comma 2)[65]. Quest'ultima è desunta dai motivi a delinquere e dal carattere del reo, dai suoi precedenti penali e dalla vita anteatta, dalla condotta contemporanea o susseguente al reato e dalle condizioni di vita individuale, familiare e sociale. Come si vede, si tratta di fattori sovrapponibili a quelli utilizzati per la valutazione algoritmica del rischio di recidiva nel sistema americano[66].

In linea di principio esisterebbe quindi un addentellato normativo cui ancorare l'utilizzo di strumenti a supporto delle decisioni del giudice nell'applicazione della pena. Tuttavia, l'utilizzo di questi strumenti rischierebbe di collidere con alcuni basilari principi del processo penale.

Deve anzitutto rilevarsi come, diversamente dal modello americano, nel nostro ordinamento non esiste alcuna distinzione bifasica tra pronuncia della sentenza di condanna e successiva irrogazione della pena, e tantomeno una fase intermedia di istruttoria sulla personalità del reo. Seppur esistesse o si affermasse questo particolare *modus procedendi,* il principio di formazione della prova nel contraddittorio delle parti (art. 111, comma 4, Cost.) dovrebbe ragionevolmente impedire al giudice di acquisire autonomamente elementi utili ai fini della commisurazione della pena, o di valutare elementi diversi da quelli oggetto di contraddittorio tra le parti. L'attivazione di poteri istruttori *ex officio*, o anche su istanza di parte, sarebbe altresì preclusa dal disposto dell'art. 220, comma 2, del codice di rito, dove lapidariamente si afferma che, salvo quanto previsto ai fini dell'esecuzione della pena o della misura di sicurezza, «non sono ammesse perizie per stabilire l'abitualità o la professionalità nel reato, la tendenza a delinquere, il carattere e la personalità dell'imputato e in genere le qualità psichiche indipendenti da cause patologiche». Ne deriva, *de iure condito,* l'impossibilità di utilizzare strumenti come COMPAS che si basano sulle risposte fornite dall'imputato al consulente incaricato, a meno di non voler eludere i divieti stabiliti dalla legge[67]. Una attività di questo tipo, anche se diversamente denominata, integrerebbe a tutti gli effetti una perizia e, come tale, inutilizzabile per violazione di legge *ex* art. 191, comma 1, c.p.p. Proprio negli anni in cui la prassi giudiziaria americana iniziava a confrontarsi con l'idea dell'*evidence-based sentencing*, il legislatore del nuovo codice di procedura penale Vassalli rifiutava apertamente l'idea di una istruttoria sulla capacità a delinquere del reo. Che il divieto dettato per la perizia fosse stato concepito anche in funzione dell'applicazione della pena[68], risulta in modo abbastanza chiaro dalle parole del legislatore. L'art. 220 c.p.p. indica infatti alcuni degli elementi che il giudice dovrebbe tenere in considerazione ai sensi del secondo comma dell'art. 133 c.p., escludendo che possano compiersi su di essi accertamenti di carattere tecnico-scientifico. È stato osservato[69] che tale impostazione ribaltava l'orientamento favorevole[70] alla perizia avente ad oggetto la personalità

[65] Secondo la dottrina più autorevole, i due commi che compongono l'art. 133 c.p. rappresentano un compromesso tra scuola classica e scuola positiva del diritto penale: la prima incline ad ammettere il carattere etico-retributivo della pena (il reo deve essere punito per ciò che ha commesso), la seconda a riconoscerne la funzione meramente incapacitante (il reo deve essere allontanato dalla società poiché pericoloso). In argomento, Antolisei (2003), p. 722; Dolcini (1979); Pagliaro (1981), p. 25; Militello (1982); Bricola (1965).

[66] Fatta eccezione per la condotta contemporanea o successiva al reato, gli altri sono fattori che facilmente possono essere generalizzati a livello statistico e rese disponibili in forma di dati.

[67] Si potrebbe ritenere che la semplice intervista all'imputato non sia una attività riconducibile alla perizia. Tale tesi si scontrerebbe tuttavia con il dato testuale della legge, secondo cui si ha perizia quando «*occorre svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze tecniche, scientifiche*» (art. 220, comma 1, c.p.p.). Nel caso in esame l'attività demandata al consulente è rivolta ad ottenere informazioni per acquisire dati e valutazioni di natura tecnica, e rientra appieno della definizione codicistica.

[68] Il tenore del divieto non include la fase dell'esecuzione della pena, per cui sarebbe astrattamente possibile che il magistrato o il tribunale di sorveglianza, per le decisioni rispettiva competenza, utilizzino strumenti attuariali di valutazione del rischio senza incorrere nell'elusione o della violazione del divieto in esame.

[69] In argomento v. l'approfondimento di Martucci (2004), p. 746, dal quale abbiamo tratto importanti spunti bibliografici per ricostruire il dibattito sul tema della perizia criminologica nel processo penale.

[70] Nel progetto del nuovo codice di procedura penale, elaborato dalla Commissione ministeriale presieduta da Giandomenico Pisapia (c.d. Progetto Pisapia) la perizia criminologica diveniva un importantissimo strumento diagnostico di cui il giudice poteva avvalersi ogni qualvolta, nella fase della cognizione, avesse dovuto formulare un giudizio sulla personalità e sulla pericolosità sociale del reo. L'art. 209, comma 2, del Progetto preliminare prevedeva infatti che «*Ai fini del giudizio sulla personalità e pericolosità, la perizia può avere ad oggetto la personalità dell'imputato anche in ordine alle qualità psichiche indipendenti da cause patologiche*». Il successivo art. 212 comma 2, statuiva inoltre che: «*Le perizie relative ai quesiti sulla personalità e pericolosità sono affidate a specialisti in criminologia ovvero ad un medico specialista in psichiatria o*

e le condizioni psichiche dell'imputato che sembra animare la legge delega all'emanazione del nuovo codice di procedura penale[71]. Parte autorevole della dottrina giuridica e medico-legale accoglieva con favore l'impostazione del nuovo codice, osservando come il rigido limite imposto alla perizia fosse destinato ad evitare l'inattendibilità scientifica di una verifica sulla personalità dell'imputato, in considerazione della oggettiva labilità dell'indagine e dell'atteggiamento condizionato del periziando[72], e del rischio di violazione del diritto di difesa laddove, limitando la libertà psico-fisica dell'imputato, potrebbero facilmente essere aggirate le garanzie e gli strumenti tipici per l'acquisizione della prova[73]. È curioso notare come alcuni autori[74] abbiano giustificato il divieto facendo riferimento – *ex adverso* – al disposto dell'art. 133 c.p. che, rimettendo alla piena discrezionalità al giudice la commisurazione della pena, sarebbe sintomatico della volontà del legislatore codicistico di sottrarre campo alle possibili evidenze scientifiche sulla personalità del reo.

Per temperare il rigore delle posizioni più estremiste, alcuni autori[75] proposero una terza via, quella della c.d. *istruttoria bifasica*, che ricorda il modello statunitense pocanzi esaminato[76]. La distinzione tra fasi dell'istruttoria farebbe venir meno il pericolo che la perizia criminologica possa trasformarsi in uno strumento da utilizzare contro lo stesso imputato: se l'indagine fosse espletata prima dell'accertamento della penale responsabilità del reo sarebbe eluso il principio di presunzione d'innocenza (art. 27 Cost.); viceversa in un processo caratterizzato da una prima fase riservata all'accertamento della responsabilità dell'imputato e da una seconda destinata alla scelta del trattamento individualizzato (nel quale collocare l'indagine criminologica), non vi sarebbe alcun rischio di "inquinare" l'istruttoria sull'*an* della responsabilità con elementi di prova concernenti il *quantum puniatur.*

4.1. *Probabilità statistica e pericolosità sociale.*

Tanto premesso, sia pur sinteticamente, sulle posizioni emerse in dottrina, possiamo osservare come i limiti imposti dal legislatore alla perizia non escludano del tutto la possibilità di una valutazione algoritmica della pericolosità del reo. Rimane infatti aperta la possibilità di utilizzare strumenti predittivi che, basandosi unicamente su dati statistici o su informazioni personali disponibili (quali i precedenti penali, la composizione del nucleo familiare, la località di residenza, il grado di scolarizzazione), permettono di esprimere un giudizio ipotetico sulla futura capacità a delinquere.

Ci si sente tuttavia di esprimere qualche dubbio circa l'attendibilità di tali strumenti. Il punteggio di rischio verrebbe in tal modo calcolato incrociando i dati relativi a situazioni simili o vicende analoghe, facendo cadere il giudizio sulla pericolosità sociale del reo in un labirinto di inevitabili generalizzazioni empiriche. Né del resto sarebbe possibile una individualizzazione del giudizio mediante l'inserimento in i*nput* di informazioni dettagliate sulla personalità dell'imputato, stante il generale divieto espresso dal secondo comma dell'art. 220 c.p.

Si potrebbe però obiettare che la valutazione basata su evidenze statistiche può, a seconda del campione di riferimento, essere molto affidabile; oppure, più semplicemente, che il diritto

psicologia». In quel tempo l'utilità della perizia criminologica era riconosciuta anche da autorevoli penalisti, tra cui il Mantovani (1988), p. 670.

[71] L'art. 2, comma 1, n. 10 della legge 3 aprile 1974, n. 108 prevedeva, tra i principi e criteri direttivi, che il delegato dovesse provvedere *«al riordinamento dell'istituto della perizia, con particolare riferimento alla perizia medico-legale, psichiatrica e criminologica, assicurando la massima competenza tecnica e scientifica dei periti»*. L'espresso riferimento alla perizia criminologica è un chiaro segnale del *favor* espresso dal legislatore per l'indagine sulla personalità dell'imputato. Il principio era verosimilmente stato inserito poiché il legislatore intendeva "rompere" con la tradizione, atteso che il precedente codice di procedura penale del 1930 sanciva all'art. 314, comma 2, un divieto molto simile a quello oggi contenuto nell'art. 200, comma 2. L'originaria formulazione del codice di procedura penale
configurava un processo definito dalla dottrina "quasi impermeabile" agli apporti delle scienze non giuridiche. Cfr. Amodio (1989), p. 58; Martucci (2004), p. 744, il quale ricorda che nel sistema previgente si erano poste diverse questioni di legittimità costituzionale per contrasto con gli artt. 27 comma 3, e 3 Cost., sull'argomentazione che il divieto della "perizia di personalità" confliggeva con il principio della finalità rieducativa della pena, indebolendo di fatto il diritto alla difesa per l'imputato e determinava un trattamento differenziato fra imputati maggiorenni e minorenni. Tuttavia, la Corte Costituzionale si espresse sempre riconoscendo la conformità dei divieti contestati ai principi costituzionali (Corte Cost. 9 luglio 1970, n. 124, in *Riv. pen.*, 1970, II, 684; Corte Cost. 19 dicembre 1973, n. 179, in *Giust. pen.*, 1974, I, 72).

[72] Di quest'avviso, Pannain *et al.* (1989), p. 848.

[73] Cordero (1986), p. 347; Ramajoli (1995) p.159

[74] Perchinunno, (2008), p. 224; Giannitti (2005), p. 199.

[75] Rivello (1995), p. 479; Bielli (1991), p. 65.

[76] Si veda *supra,* § 2.2.

penale si affida spesso a giudizi di questo tipo (basti pensare al concetto di probabilità statistica e alle moderne teorie sul rapporto giuridico di causalità)[77].

A nostro avviso tale critica non coglierebbe nel segno. La prognosi sulla capacità a delinquere è un giudizio *intuitu personae*, strettamente legato alla personalità del reo[78]: nessuna risultanza statistica sarà mai in grado di avvalorare da sé un giudizio positivo o negativo sulla pericolosità sociale. Il campione di dati sulla cronistoria delinquenziale di certo luogo è ottenuto raggruppando i criminali per fasce d'età, zone di residenza, situazione familiare etc. Un individuo potrebbe così essere considerato a rischio di recidiva soltanto in virtù dell'appartenenza a un gruppo: ciò produrrebbe l'indesiderato effetto di "contaminare" la valutazione discrezionale del magistrato senza fornire alcun elemento utile a desumere la capacità a delinquere del colpevole.

De lege lata, ci sembra di dover concludere nel senso della inopportunità dell'utilizzo degli algoritmi predittivi nel processo penale. I limiti imposti alla perizia criminologica ammetterebbero unicamente una valutazione basata su indici di rischio presuntivi, del tutto inidonei ad orientare la discrezionalità giudiziaria nella commisurazione della pena.

4.2. L'aemulatio *del modello statunitense. I vantaggi di una valutazione algoritmica di tipo misto.*

Esaminando cursoriamente il funzionamento dei *software* predittivi nel sistema giudiziario americano[79], abbiamo detto che essi di basano per lo più su un algoritmo di ponderazione di diversi fattori: non solo il *dataset* relativo a profili di criminali ritenuti "simili" a quello dell'imputato, ma anche le risposte fornite da questi nel corso dell'interrogatorio. I più recenti approdi giurisprudenziali delle corti statunitensi[80] valorizzano proprio questo momento "individualizzante" per frugare i dubbi di una possibile violazione del *right to an individualized sentence*. Il punteggio di rischio calcolato dalla macchina è il risultato di una valutazione di tipo misto, che tiene conto non solo delle statistiche generali, ma anche del profilo criminologico dell'imputato ricostruito in base ai risultati del questionario. La risposta dell'algoritmo ha una funzione soltanto orientativa delle scelte del magistrato[81], che rimane libero di decidere se attenersi o meno all'indice di pericolosità calcolato e, nel caso in cui lo condivida, se sia per ciò opportuno determinare la pena base in misura maggiore.

A nostro modo di vedere, un sistema così strutturato – che permetta al giudice di attingere dagli esiti di una valutazione algoritmica di tipo misto, previa adozione di tutte le cautele necessarie per assicurare il rispetto delle garanzie difensive dell'imputato[82] – sarebbe degno di considerazione anche nell'ordinamento processuale italiano. Un primo passo in questa direzione dovrebbe essere compiuto ripensando il divieto di perizia criminologica che, nel quadro normativo vigente, rappresenta l'ostacolo più significativo all'utilizzo degli algoritmi predittivi.

Il limite contenuto al secondo comma dell'art. 220 c.p.p. esprime chiaramente la diffidenza del legislatore nei confronti del modello basato sull'*evidence based sentencing*, che, in realtà, ci sembra di gran lunga preferibile rispetto a quello della discrezionalità pura. Si possono addur-

[77] Il ragionamento esplicativo di eliminazione mentale in tanto può essere effettuato in quanto si conosca in precedenza che da una certa azione scaturisce o non scaturisce un certo evento, conoscenza che può derivare immediatamente dalla scienza; tuttavia, ove quest'ultima non soccorra, deve poter essere acquisita *aliunde*. Secondo gli insegnamenti di Stella, (2001) p. 183, un antecedente può essere configurato come condizione necessaria solo a patto che esso rientri nel novero di quegli antecedenti che, sulla base di una successione regolare conforme a una legge dotata di validità scientifica, portano ad eventi del tipo di quello verificatosi in concreto. Tali leggi generali possono essere sia quelle *universali*, in grado di affermare che la verificazione di un evento è invariabilmente accompagnata dalla verificazione di un altro evento, sia le leggi *statistiche* che si limitano, invece, ad affermare che il verificarsi di un evento è accompagnato dal verificarsi di un altro evento soltanto in una certa percentuale di casi, con la conseguenza che questi ultimi sono tanto più dotati di validità scientifica quanto più possono trovare applicazione in un numero sufficientemente alto di casi e di ricevere conferma mediante il ricorso a metodi di prova razionali e controllabili.

[78] Esiste una marcata differenza tra la regolarità causale naturalistica e il giudizio ipotetico sul futuro comportamento di un individuo: le risultanze statistiche a supporto della prima permettono di affermare con un alto grado di probabilità logica e di credibilità razionale che a determinate condizioni seguirà un certo evento; il campione di dati sul tasso di recidiva nel reato non è invece sufficiente a comprovare alcunché, potendo ben darsi che un soggetto potenzialmente pericoloso si astenga poi dal commettere reati.

[79] *Amplius*, § 2.2

[80] Wisconsin Supreme Court, S*tate v. Loomis*, cit., § 46 ss (*supra,* § 3.1.).

[81] Anche nelle giurisdizioni in cui l'utilizzo degli strumenti di *risk assessment* è obbligatorio, il giudice conserva piena discrezionalità nella commisurazione della pena. Alcuni autori hanno prontamente rilevato come l'esercizio potere discrezionale dovrebbe trovare adeguato riscontro nella motivazione della sentenza. v. Kehl *et al.* (2017), p. 20

[82] *Amplius,* § 5.

re al riguardo almeno due ragioni.

Anzitutto, l'umana impossibilità di ponderare in modo accurato tutti gli indici sintomatici della capacità a delinquere del reo (art. 133, comma 2, c.p.), quali il carattere, la vita anteatta, le condizioni di vita individuale, familiare e sociale. La valutazione giudiziale su questi elementi si risolve il più delle volte in una prima "impressione", positiva o negativa, sulla personalità dell'imputato, condizionata dall'esistenza di precedenti penali che risultano dal certificato del casellario. Per conoscere compiutamente del carattere e della personalità del reo il giudice dovrebbe disporre di mezzi istruttori vietati[83], in mancanza dei quali non gli rimane che affidarsi a elementi di "pronta soluzione" (condanne passate in giudicato, circostanze di fatto emerse nel corso dell'istruttoria o di comune esperienza) dai quali ritiene possa desumersi la capacità a delinquere secondo un ragionamento di tipo induttivo-presuntivo. Il metodo utilizzato non assicura l'oggettività di giudizio, essendo questo condizionato dai soli elementi che il giudice ha voluto valorizzare tra quelli che aveva a disposizione. L'impiego di strumenti e tecniche di valutazione algoritmico-attuariale del rischio di tipo "misto" renderebbe certamente più obiettiva l'analisi, offrendo al giudice una valida guida per orientare l'esercizio del potere discrezionale. Non solo verrebbero ad essere considerati alcuni indici tendenzialmente negletti (come il carattere e la personalità individuale del reo), ma anche quei fattori sociali dei quali non si conosce *a priori* la possibile efficacia condizionante (luogo di residenza, composizione familiare etc)[84].

Il modello dell'*evidence based sentencing* si lascia preferire anche per la fiducia che attribuisce alla valutazione scientifica della personalità del reo. Come noto, il diritto penale ha mostrato una progressiva apertura alla diagnostica psicologica, che oggi assume un rilievo centrale per l'accertamento di alcune fattispecie di reato[85]. Il progresso compiuto dalle scienze psicologiche negli ultimi anni dovrebbe condurre a un ripensamento dell'atteggiamento di chiusura finora mostrato, non più giustificabile sulla base dell'asserita scarsa valenza scientifica nel metodo e dei risultati ottenuti. Del resto, nel processo penale la scienza non viene in considerazione come un dato incontrovertibile, ma come un insieme di conoscenze razionali sia pur probabilistiche[86]. Pur essendo indubbia la valenza soltanto probabilistica di una indagine sulla personalità dell'imputato, i risultati della valutazione sarebbero comunque più obiettivi di quelli ricavabili da un ragionamento di tipo presuntivo.

Tali considerazioni ci inducono a credere che il progresso scientifico e tecnologico abbia reso ormai obsoleto il *modello della discrezionalità pura* nella commisurazione della pena, che dovrebbe cedere di fronte a un *modello di discrezionalità "condizionata"*[87].

5. Quali garanzie per il rispetto del diritto di difesa? I possibili lineamenti di un modello di discrezionalità "condizionata" nella commisurazione della pena.

Nell'esprimere una opinione certamente favorevole all'introduzione di strumenti di valutazione statistico-attuariale per la commisurazione della pena, appare più che doveroso porre l'accento sulla necessità di assicurare il rispetto delle garanzie difensive dell'imputato.

Il dibattito sorto sull'utilizzo degli algoritmi predittivi nell'ordinamento nordamericano e, più in generale, l'esperienza maturata all'indomani della riforma del *sentencing*[88], ci porta a

[83] Oltre alla perizia criminologica, che come si è più volte ribadito non è ammessa ai fini della commisurazione della pena, viene in rilievo anche il limite all'integrazione istruttoria d'ufficio (art. 507 c.p.p.), ammessa solo quando risulti assolutamente necessario. A nostro avviso non ricorrerebbe tale esigenza nel caso in cui mancasse la prova su uno degli elementi dell'art. 133 c.p., tenuto conto anche del rischio di elusione del divieto posto dall'art. 220 c.p.p., qualora il giudice potesse, ad esempio, acquisire d'ufficio la cartella clinica-psicologica oppure chiamare come testimone lo psicanalista dell'imputato.

[84] Sono questi elementi che possono essere desunti dalle statistiche elaborate a livello regionale o nazionale, poste alla base del funzionamento degli algoritmi predittivi negli ordinamenti nazionali statunitensi (cfr. *supra*, 2.2).

[85] Ci si riferisce agli eventi caratterizzanti il delitto di atti persecutori, c.d. *stalking* (art. 612-*bis* c.p.) e di tortura (art. 613-*bis* c.p.).

[86] Di questo avviso, Canzio (2017) pp. 3-19; Canzio (2018), p. 4, il quale parla dell'accertamento giudiziale come arte del giudicare «*reasonig under uncertainty*», sia pur «*by probabilities*».

[87] Per la concreta attuazione di un tale modello il legislatore dovrebbe intervenire sulle disposizioni del codice di rito introducendo un espresso riferimento alla possibilità di utilizzare strumenti e tecniche di valutazione del rischio, previa abolizione dei limiti alla perizia crininologica. Al riguardo, sarebbe sufficiente introdurre in apertura dell'art. 220, comma 2 c.p.p. un espresso riferimento alla commisurazione della pena tra le attività per le quali è essa è consentita.

[88] *Amplius,* v. § 2.1

riflettere sulle cautele da adottare per costruire un modello di discrezionalità condizionata nel processo penale italiano. Si impone, in particolare, l'osservanza di un triplice ordine di garanzie, relative al *modus procedendi* e al consenso dell'imputato, al tipo di strumento da utilizzare e all'onere di motivazione in capo al giudice.

Quanto alle prime, è da accogliere con favore la distinzione bifasica tra istruttoria precedente e successiva alla sentenza di condanna. Se le valutazioni sulla personalità del reo fossero acquisite prima della chiusura del dibattimento si profilerebbe il pericolo – tutt'altro che infondato – di "inquinamento" della decisione finale sulla base delle risultanze del *risk assessment*[89]. Seguendo l'esempio statunitense si potrebbe introdurre l'istituto della condanna generica, con cui il giudice – all'esito del dibattimento[90], ritenendo l'imputato colpevole del fatto addebitatogli – dispone gli opportuni mezzi istruttori finalizzati alla decisione sulla pena da irrogare al caso concreto. In ogni caso, si ritiene che, in ossequio al diritto al silenzio e al generale *privilege against self-incrimination* l'indagine sulla personalità possa essere disposta unicamente con il consenso dell'imputato, in mancanza del quale il giudice dovrà procedere nei modi ordinari alla applicazione della pena.

Particolari accorgimenti sono poi necessari nella scelta dello strumento e delle tecniche da utilizzare per la valutazione del rischio. Le criticità emerse nel sistema americano dimostrano l'importanza di una completa *disclosure* degli indici di valutazione e dei fattori di ponderazione utilizzati. Nella fase istruttoria *post* condanna, la difesa deve essere messa in condizione di conoscere il peso attribuito ai diversi fattori e di verificare la ragionevolezza dei parametri utilizzati, nonché la correttezza della valutazione finale. L'accertamento tecnico dovrebbe essere eseguito nel rispetto del principio del contraddittorio (art. 111, comma 2, Cost.): il giudice, nella sua veste di *peritus peritorum,* potrà così esperire un controllo sull'utilizzo di metodi dotati di una certa affidabilità, prendendo posizione sulle obiezioni sollevate dalle parti. Non può tuttavia essere taciuto come l'attuazione di un tale modello dipenda, per larga parte, dall'esistenza di validi strumenti di *risk assessment*[91]. Soltanto la convergenza di competenze interdisciplinari tra diagnostica psicologica e criminologica, scienze attuariali e tecnologia consentirà la creazione di uno strumento in grado di bilanciare razionalmente i risultati dell'indagine personale con campione di dati sufficientemente ampio.

Per quel che riguarda, infine, la decisione sul *quantum* di pena da irrogare nel caso concreto, il magistrato sarà tenuto a dar conto in motivazione dei risultati dell'*assessment* e delle ragioni per cui ritiene di doverne condividere o meno gli esiti. Il modello della discrezionalità condizionata consente l'ingresso nella dialettica processuale di elementi di valutazione più oggettivi, logicamente verificabili e censurabili dalle parti con gli ordinari mezzi di impugnazione[92]. Il vaglio discrezionale del magistrato elimina alla radice il rischio di un trattamento non individualizzato dovuto all'utilizzo delle risultanze statistiche. Egli sarà infatti tenuto a valutare criticamente tanto l'attendibilità del punteggio di rischio, quanto le obiezioni sollevate dal difensore e dal pubblico ministero, con possibilità di discostarsi dagli esiti della valutazione o di tenerne conto soltanto in parte per la determinazione della pena da applicare al caso concreto. Un sistema così strutturato permetterebbe di "assorbire" nel vivo della dialettica processuale e della motivazione della sentenza di condanna le questioni e i dubbi relativi allo strumento utilizzato per valutare la capacità a delinquere del reo.

6. Conclusioni. *Iudex ex machina* tra mito e realtà.

Alla luce delle esposte considerazioni, ci chiediamo se l'ingresso dei *Big Data* e delle tecnologie *smart* nel processo penale possa essere davvero considerato un valore aggiunto al modello

[89] Gli esiti della valutazione potrebbero infatti produrre un effetto condizionante notevole sulla decisione. Nel dubbio circa la colpevolezza dell'imputato, qualsiasi giudice sarebbe indotto (o quantomeno più propenso) a condannare un soggetto ritenuto socialmente pericoloso e ad alto tasso di recidiva.

[90] Il legislatore dovrebbe ovviamente prevedere gli opportuni adeguamenti normativi nel caso in cui la sentenza di condanna sia pronunciata all'esito di giudizio abbreviato e disporre la possibilità di una istruttoria sulla personalità anticipata all'udienza preliminare nel caso in cui le parti richiedano l'applicazione di una pena ai sensi degli artt. 444 ss. c.p.p.

[91] Un simile *software* non potrà essere coperto da alcun diritto di proprietà industriale, dovendo piuttosto essere "trasparente" nel suo funzionamento.

[92] In un sistema dominato dalla discrezionalità pura nella commisurazione della pena raramente saranno disponibili elementi oggettivi per confutare la valutazione espressa dal magistrato sulla capacità a delinquere del colpevole.

adversary del contraddittorio. La risposta al quesito è necessariamente relativa, non potendo prescindere dall'esame delle scelte compiute dal legislatore. Egli dovrà anzitutto considerare i fini da perseguire attraverso l'utilizzo dei nuovi ritrovati tecnologici, selezionando soltanto quelli che siano compatibili con le esigenze proprie del rito penale. Non sarebbe ad esempio giustificabile la sostituzione dell'attività umana all'esclusivo fine di migliorare l'efficienza o la rapidità della giustizia; sarebbero al contrario meritevoli di attenzione quelle tecnologie che assicurano una più accurata gnoseologia processuale o garantiscono l'accesso a conoscenze altrimenti indisponibili[93]. Il legislatore dovrà poi apprestare i mezzi più adeguati a garantire che l'ingresso della tecnologia non stravolga i principi e le garanzie del processo penale.

Avuto riguardo alla attività del giudice nella commisurazione della pena si ritiene che l'ingresso dei *software* predittivi renda possibile una prognosi più accurata della capacità a delinquere del reo e la valutazione dei singoli parametri indicati al secondo comma dell'art. 133 c.p. Si tratta di un fine certamente auspicabile, che dovrà tuttavia essere perseguito attraverso mezzi idonei a preservare le garanzie tipiche del processo penale. Particolare cautela dovrà essere prestata nella selezione dei soli strumenti predittivi che confrontino i risultati dell'esame individuale con le statistiche relativi a profili criminologici analoghi (strumenti di valutazione c.d. di tipo misto). L'apporto della diagnostica psicologica assicura una adeguata individualizzazione del trattamento e, soprattutto, permette di superare le censure relative ai possibili effetti discriminatori dati dall'appartenenza dell'individuo a un particolare profilo criminologico[94].

Il rispetto del diritto di difesa e dei principi del giusto processo presuppone che l'indagine sulla personalità del reo sia svolta, previo consenso di questi, secondo i dettami del contraddittorio processuale. L'attuazione di un modello di *discrezionalità condizionata* nella commisurazione della pena è possibile soltanto distinguendo l'istruttoria sull'*an* della responsabilità da quella sul *quantum* di pena ed estendendo a questa seconda fase le medesime garanzie di formazione della prova "tecnica" previste per la prima[95]. A monte il legislatore dovrebbe ammettere la possibilità di utilizzare unicamente strumenti dei quali sia noto il funzionamento e il peso attribuito ai fattori di *input;* la trasparenza rappresenta un elemento fondamentale per incardinare il contraddittorio processuale sui risultati della valutazione del rischio.

Si ritiene che il timore legato all'utilizzo di metodi privi di validazione scientifica (probabilistici o non scientificamente dimostrabili) possa essere superato grazie agli strumenti della dialettica processuale. Il giudice dovrà infatti motivare sui risultati della valutazione, sull'attendibilità del punteggio di rischio calcolato dalla macchina e sulle obiezioni sollevate dalle parti, in modo da consentire una ricostruzione dell'*iter* logico-motivazionale alla base della determinazione della pena

Il progressivo perfezionamento dei *software* di valutazione attuariale del rischio diverrà, nel prossimo futuro, un utile incentivo per superare il "mito" della discrezionalità giudiziaria pura nella commisurazione della pena. Occorre infatti ribadire l'opportunità politico criminale di una valutazione effettiva – e non meramente stilistica – sulla capacità a delinquere del colpevole, resa estremamente difficoltosa dall'impossibilità di disporre indagini psicologiche o criminologiche (art. 220, comma 2, c.p.p.). La possibilità per il giudice penale di utilizzare strumenti di *risk assessment* apre orizzonti nuovi anche rispetto alle decisioni, ben più delicate, sul pericolo di reiterazione del reato per l'applicazione delle misure cautelari personali (art. 274, comma 1, lett. c) c.p.p.) o per la loro revoca o sostituzione (art.. 299 c.p.p.), per la concessione del beneficio della sospensione condizionale della pena (art. 164 c.p.), oppure di misure alternative alla detenzione carceraria (art. 53,55 e 56 l. 689/1981) o di misure di sicurezza non detentive (art. 228 c.p.).

Quale che sia l'ambito processuale di applicazione, sarebbe errato parlare di *iudex ex machina*: non si tratta qui di automatizzare una attività di esclusiva competenza del magistrato, quanto piuttosto di rendere più agevole un giudizio prognostico per sua natura molto complesso.

In conclusione, l'auspicio per il futuro è che il legislatore prenda coscienza delle opportunità offerte dal modello dell'*evidence based sentencing* e inizi a riflettere sulla possibilità di aprire le porte ai nuovi ausiliari tecnologici nel processo penale.

[93] Al riguardo basti pensare alle enormi potenzialità offerte dalla tecnologia per l'acquisizione della prova tramite mezzi atipici (es. pedinamenti virtuali, intercettazioni di flussi telematici, *open source intelligence*, *blood pattern analysis* etc.).
[94] *Amplius*, v. § 4.1.
[95] Cfr. art. 190, 220 ss., 501, 508 c.p.p.

Bibliografia

Amodio, Ennio (1989): "Perizia e consulenza tecnica nel quadro problematico del nuovo processo penale", *Cassazione penale,* p.158

Antolisei, Francesco (2003): *Manuale di diritto penale - Parte generale*, (Milano, Giuffrè)

Bennett Moses, Lyria, Chan, Janet (2018): "Algorithmic prediction in policing: assumptions, evaluation, and accountability", *Policing and society,* 28, 7, pp. 806-822

Bielli, Daniele (1991): "Periti e consulenti tecnici nel nuovo processo penale", *Giustizia penale,* p. 65

Bonczar, Thomas (2003): "Prevalence of Imprisonment in the US Population, 1974-2001" (U.S. Department of Justice, https://www.bjs.gov/)

Bricola, Franco (1965): *La discrezionalità nel diritto penale*, (Milano, Giuffrè)

Cannata, Salvatore (2002): "La commisurazione della pena nel sistema federale statunitense", *Rivista del Centro di ricerca interuniversitario su carcere, devianza, marginalità e governo delle migrazioni* (https://adir.unifi.it)

Canzio, Giovanni (2017), "La motivazione della sentenza e la prova scientifica: "reasoning by probabilities", in Canzio, Giovanni, Luparia, Luca (editor): *Prova scientifica e processo penale*, (Padova,Cedam), pp. 3-19

Canzio, Giovanni (2018): "Il dubbio e la legge", *Diritto penale contemporaneo,* 20 luglio 2018

Cohen, Jacqueline (1983): "Incapacitation as a Strategy for Crime Control: Possibilities and Pitfalls, in Crime and Justice", *University of Chicago Journals – Crime and Justice,* 5, I, pp. 1-84

Cordero, Franco (1986): *Guida alla procedura penale,* (Torino, UTET)

Davis, Kennett Culp (1969): *Discretionary Justice: A Preliminary Inquiry* (Baton Rouge, Louisiana State University Press)

Dolcini, Emilio (1979): *La commisurazione della pena,* (Padova, CEDAM)

Faigman, David, Monahan, John (2005): "Psychological Evidence at the Dawn of Law's Scientific Age", *Annual Review of Psychology*, 56, pp. 631-659

Frankel, Marvin (1972), *Criminal Sentences: Law without Order*, (New York, Hill and Wang)

Gianniti, Pasquale (2005): *La valutazione della prova penale*, (Torino, UTET)

Hartcourt Bernard (2005): "Against Prediction: Sentencing, Policing and Punishing in an Actuarial Age", *University of Chicago Public Law & Legal Theory Working Paper*, 94

Kehl, Danielle, Guo, Priscilla, Kessler, Samuel (2017): "Algorithms in the Criminal Justice System: Assessing the use of Risk Assessments in Sentencing", *Responsive Communities Initiative, Berkman Klein Center for Internet and Society* (Harvard Law School, https://dash.harvard.edu)

Klingele, Cecelia (2016): "The Promises and Perils of Evidence-Based Corrections", *Notre-Dame Law Review*, 91, II, pp. 537-584

Mantovani, Ferrando (1988): *Manuale di diritto penale*, (Padova, CEDAM)

Martucci, Pierpaolo (2004): "Il contributo del criminologo nel processo penale: un problema ancora aperto", *Diritto penale e processo,* 6, pp. 744-749

Mathiesen, Thomas (1998): "Selective Incapacitation Revisited", *Law and Human Behavior,* 22, 4, pp. 455-469

Militello, Vincenzo (1982): *Prevenzione generale e commisurazione della pena*, (Milano, Giuffrè)

Montesquieu, Charlès Louis de Secondàt (1798): *De l'esprit des loix,* (Geneve)

Pagliaro, Antonio (1981): "Commisurazione della pena e prevenzione generale", in *Rivista italiana di diritto e procedura penale,* pp. 25-38

Pannain, Bruno, Albino, Marcello, Pannain, Mario (1989): "La perizia sulla personalità del reo: evoluzione dottrinaria e normativa. Prospettive nel c.p.p. '88", *Rivista italiana di medicina legale*, pp. 848-863

Perchinunno, Vincenzo (2008): "Le prove", in Pisani, Mario et a. (editor): *Manuale di procedura penale*, (Bologna, Monduzzi), pp. 265-286

Ramajoli, Sergio (1995): *La prova nel processo penale*, (Padova, CEDAM)

Redding, Richard (2009), "Evidence-Based Sentencing: The Science of Sentencing Policy and Practice", *Chapman Journal of Criminal Justice*, 1, pp. 1-19

Rivello, Paolo (1995): "Perito e perizia", *Digesto delle discipline penalistiche*, IX, pp.474-480

Singh, Jay, Kroner, Daryl, Wormith, Stephen, Desmarais, Sarah, Hamilton, Zachary (2018): *Handbook of Recidivism Risk/Needs Assessment Tools*, (Hoboken, Wiley-Blackwell)

Starr, Sonja (2014): "Evidence -based Sentencing and the Scientific Rationalization of Discrimination", *Stanford Law Review*, 66, pp. 803-872

Stella, Federico (2001): *Leggi scientifiche e spiegazione causale del diritto penale*, (Milano, Giuffrè)

Sum, Andrew (2009): "The Consequences of Dropping Out of High School: Joblessness and Jailing for High School Dropouts and the High Cost for Taxpayers", *Center for Labor Market Studies at Northeastern University,* Paper 23

Teubner, Gunther (2018): *Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten*, *Ancilla Iuris*, pp. 106-149

Teubner, Gunther (2015): *Ibridi e attanti, Attori collettivi ed enti non umani nella società e nel diritto*, (Milano, Mimesis)

Thompson, James., Starkman, Gary (1974): "Reviewed Work: Criminal Sentences: Law without Order", *Columbia Law Review*, 1974, 74, I, pp. 152-158

Banche dati, attività informativa e predittività. La garanzia di un diritto penale del fatto.

Bases de datos, actividades de información y predictibilidad. La garantía de un derecho penal del hecho

Databases, Information Activities and Prediction. The Safeguard of Fact-related Criminal Law

Pietro Sorbello
sorbello.pietro@gdf.it

Xxxx Xxxx Xxxx

Abstracts

L'impiego elettivo degli algoritmi predittivi riguarda oggi la prevenzione dei reati, in particolare l'attività di polizia. Le nuove tecnologie consentono di analizzare e confrontare dati, restituendo una sintesi di informazioni complesse per orientare le attività di prevenzione: alla tradizionale ricerca della notizia di reato, si affianca ormai anche l'analisi dei metadati, cioè del sistema delle relazioni fra dati singolarmente non significativi.
L'obiettivo del lavoro è esaminare, nella prospettiva dell'efficacia dei controlli, la disciplina che, per le analisi del rischio di evasione, consente l'accesso all'archivio dei rapporti finanziari e l'utilizzabilità delle informazioni rilevanti ai fini della disciplina antiriciclaggio

La utilización de algoritmos predictivos está actualmente relacionada con la prevención de los delitos, en particular con la actividad de policía. Las nuevas tecnologías permiten analizar y confrontar datos, restituyendo una síntesis de informaciones complejas para orientar las actividades de prevención: a la tradicional investigación de casos para ser reportados, se añade hoy el análisis de metadatos, es decir, el estudio de correlaciones entre datos individualmente no significativos. El objetivo del artículo es examinar la regulación que, ante un posible caso de evasión, consiente el acceso al archivo de las relaciones financiarías y el uso de dicha información.

The usage of predictive algorithms mainly refers to crime prevention, such as the police activity. New technologies allow data analysis and comparison, in order to obtain a summary of complex information used to address crime prevention: in addition to the research of cases to be reported, also metadata analysis (i.e. the correlation of data not relevant as single items) is now commonly used. The objective of the paper is to analyse the regulation which, when there is a risk of evasion, it is allowed to access the financial transactions archive, as well as the AML database.

Sommario

1. Premessa.

In un'ipotetica società distopica, disciplinata da un diritto penale illiberale, come delineata nel 1956 da Philip Dick nel racconto "*The Minority Report*", la prevenzione del reato si spinge a richiedere la sanzione penale anche per un fatto non ancora commesso, ma che è stato preconizzato. Per una simile giustizia predittiva, infatti, anche la mera intenzione costituisce reato ed apre direttamente le porte del carcere o, nella migliore delle ipotesi, consente di sottoporre a processo imputati di kafkiana inconsapevolezza.

Se il principio di materialità appresta un limite insuperabile alla responsabilità penale e la finalità rieducativa non consente di strumentalizzare l'individuo per fini generali di politica criminale, come affermato dalla Corte costituzionale in una delle sentenze "storiche"[1] per la materia penale, la predittività non è facilmente conciliabile con l'idea di giustizia penale, strettamente intesa quale giudizio sulla responsabilità penale formulato in base al libero convincimento del giudice ai sensi dell'art. 192, primo comma, c.p.p.

L'impiego elettivo degli algoritmi predittivi concerne la prevenzione dei reati, che è quell'attività della polizia di sicurezza volta ad impedire gli atti in contrasto con l'ordinamento giuridico o comunque in grado di infrangere l'ordinata e sicura convivenza civile. Attraverso capacità computazionali prima inimmaginabili, è oggi possibile analizzare e confrontare dati, ottenendo una sintesi di informazioni complesse per orientare ed ottimizzare le attività di polizia (*decision making*): alla tradizionale attività informativa basata su osservazione e deduzioni, si affianca così l'analisi dei metadati, cioè delle relazioni fra dati singolarmente o anche non immediatamente significativi.

Le nuove tecnologie forniscono un irrinunciabile contributo nella prevenzione ed acquisizione della notizia di reato, che rappresenta il primo contatto tra il diritto e la procedura penale segnando il passaggio dai poteri di polizia amministrativa alle funzioni di polizia giudiziaria. Tale contributo sarà di seguito approfondito con riferimento alla materia tributaria ed all'analisi del rischio di evasione anche mediante la consultazione dell'archivio dei rapporti finanziari.

2. Attività di polizia, protezione dei dati personali ed interesse generale alla prevenzione dei reati.

Il concetto di sicurezza affonda le sue radici alle origini di ogni forma di convivenza sociale[2].

Dal momento in cui l'individuo si associa con altri nasce l'esigenza di tutelare la sopravvivenza non solo dei singoli individui, ma del loro gruppo in relazione a possibili pericoli, interni ed esterni: il fenomeno giuridico assume così rilievo quale imprescindibile insieme di regole necessarie alla pacifica convivenza della collettività.

[1] Il riferimento è a Corte cost., sent. n. 313/1990, così definita, unitamente alla sent. n. 364/1988, da Vassalli (2007) p. 170. Nell'occasione, la Corte affermò che se la finalizzazione della pena venisse orientata solo in base alle funzioni di difesa sociale e di prevenzione generale, obliterando il principio rieducativo, "si correrebbe il rischio di strumentalizzare l'individuo per fini generali di politica criminale (prevenzione generale) o di privilegiare la soddisfazione di bisogni collettivi di stabilità e sicurezza (difesa sociale), sacrificando il singolo attraverso l'esemplarità della sanzione. È per questo che, in uno Stato evoluto, la finalità rieducativa non può essere ritenuta estranea alla legittimazione e alla funzione stesse della pena". Fiandaca (1990), p. 2385. Questa prospettiva polifunzionale costituisce un limite alla discrezionalità politica che potrà, "nei limiti della ragionevolezza, far tendenzialmente prevalere, di volta in volta, l'una o l'altra finalità della pena, ma a patto che nessuna di esse ne risulti obliterata". Così Corte cost., sent. n. 306/1993. Acconci (1994), p.861.

[2] Così Giupponi (2007). Sul concetto di sicurezza e sul rapporto con il diritto penale è stato evidenziato che "il problema della sicurezza si pone non solo come problema di sicurezza attraverso il diritto penale, ma anche come sicurezza nei confronti di quello strumento di lesione e di messa in pericolo di beni giuridici, rappresentato dal diritto e dalle istituzioni penali", Pulitanò (2009), 550. Sul tema, si vedano Donini e Pavarini (2011) nonché Risicato (2019).

Se con la nascita dello Stato moderno, la sicurezza diviene monopolio del sovrano assoluto[3], è con l'evoluzione verso lo Stato liberale di diritto che si affermano i presupposti per una visione moderna dei rapporti fra legge, libertà e governo[4]. In questa fase, prendono infatti forma i principi generali della riserva legge per le limitazioni in materia di libertà e proprietà, della rappresentanza politica e della separazione dei poteri. In netta rottura con il substrato ideologico e politico del regime assolutistico, l'individuo è posto al centro del sistema giuridico e i suoi diritti solennemente affermati nella Dichiarazione dei diritti dell'uomo e dei cittadini adottata il 26 agosto 1789.

Il rapporto tra sicurezza e diritti trova origine in questo contesto filosofico e giuridico, segue la parallela evoluzione del concetto di Stato e di legalità ed approda in seno al costituzionalismo, ove la tutela delle libertà non è più intesa come non interferenza del potere statale sulle azioni individuali, perché il ruolo dello Stato diventa anche quello di garantire i diritti individuali nella diversa prospettiva della promozione della persona, sia come singolo sia nelle formazioni sociali. Con il sorgere delle c.d. libertà positive, muta il concetto di sicurezza originariamente ancorato alla garanzia del *ne cives ad arma veniant* e delle condizioni minime della vita in comune[5].

In quest'ottica, il compito dello Stato non è limitato a reprimere comportamenti lesivi di beni giuridici, perché una garanzia effettiva dei diritti della persona passa anche attraverso interventi preventivi volti ad assicurare le condizioni per una piena espressione della persona e della sua dignità. L'ordinamento ha previsto, a tal fine, funzioni amministrative consistenti nelle "misure preventive e repressive dirette al mantenimento dell'ordine pubblico, inteso come il complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge l'ordinata e civile convivenza nella comunità nazionale, nonché alla sicurezza delle istituzioni, dei cittadini e dei loro beni"[6].

Il concetto di ordine pubblico è quindi dato "da quei beni giuridici fondamentali o da quegli interessi pubblici primari sui quali, in base alla Costituzionale e alle leggi ordinarie, si regge l'ordinata e civile convivenza dei consociati nella comunità nazionale. La tutela di questi interessi fra i quali rientrano l'integrità fisica e psichica delle persone, la sicurezza dei possessi e il rispetto o la garanzia di ogni altro bene giuridico di fondamentale importanza per l'esistenza e lo svolgimento dell'ordinamento rappresenta il nucleo delle funzioni di polizia di pubblica sicurezza [attribuite] in via esclusiva allo Stato"[7]. L'ulteriore concetto rilevante è quello di sicurezza che, al di là della sua interpretazione minima coincidente con l'incolumità fisica, descrive la situazione nella quale ai cittadini è assicurato "il pacifico esercizio di quei diritti di libertà che la Costituzione garantisce con tanta forza. Sicurezza si ha quando il cittadino può svolgere la propria lecita attività senza essere minacciato da offese alla propria personalità fisica e morale; è l'ordinato vivere civile, che è indubbiamente la meta di uno Stato di diritto, libero e democratico"[8].

Strettamente connesso alla tutela dell'ordine e sicurezza pubblica è il fine della polizia di pubblica sicurezza, individuato all'art. 1 del R.D. 18.06.1931, n. 773, di approvazione del TULPS, a norma del quale "l'autorità di pubblica sicurezza veglia al mantenimento dell'ordi-

[3] L'impianto teorico dell'assolutismo è delineato dal filosofo inglese Hobbes per il quale, attraverso il contratto sociale, gli uomini rinunciano a tutti i propri diritti naturali tranne quello alla vita, la cui salvezza è assicurata dall'ordine garantito dallo sovrano: il fine dello Stato è dunque "la pace e la difesa di tutti, e chiunque ha diritto al fine ha diritto ai mezzi", ivi compreso il potere sovrano di "fare tutto ciò che penserà sia necessario che venga fatto, sia anticipatamente per preservare la pace e la sicurezza, prevedendo la discordia all'interno e l'ostilità all'esterno, sia per riacquistare, quando si sono perdute, la pace e la sicurezza". Così Hobbes (2011), p. 177.

[4] Per il filosofo inglese John Locke "la monarchia assoluta, che da alcuni è ritenuta l'unico governo al mondo, è in contraddizione con la società civile, e dunque non può essere in alcun modo una forma di governo civile [perché] ovunque si trovino due uomini che non possono appellarsi a una legge certa e a un giudice comune sulla terra per la determinazione delle controversie di diritto tra loro, in quel caso ci si trova ancora nello stato di natura […] e così anche ogni principe assoluto rispetto a coloro che sono sotto il suo dominio", Locke (2007), p. 239 ss. Nello stesso senso, per la separazione dei poteri, si veda Montesquieu (1967), p. 207.

[5] I momenti della protezione delle libertà e della garanzia della sicurezza segnano il ruolo dello Stato in funzione strumentale *causa hominum*. Essi rappresentano anche l'eredità di un illuminismo tutto italiano, per il quale "le leggi sono le condizioni con le quali uomini indipendenti ed isolati si riunirono in società, stanchi di vivere in un continuo stato di guerra e di godere una libertà resa inutile dall'incertezza di conservarla. Essi ne sacrificarono una parte per goderne la restante con sicurezza e tranquillità e fu dunque la necessità che costrinse gli uomini a cedere parte della propria libertà ma nessuno ha voluto metterne nel pubblico deposito se non la minima porzione possibile, quella che basti ad indurre gli altri a difenderlo. L'aggregato di queste minime porzioni possibili forma il diritto di punire e tutto il di più è abuso e non giustizia, è fatto e non più diritto". Beccaria (1984), p. 25.

[6] Così l'art. 159, secondo comma, della legge 15.03.1997 n. 59, recante tra l'altro delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali.

[7] In questi termini Corte cost., sent. n. 218/1988. Per l'approfondimento si rinvia a Cerri (1990), p. 1.

[8] Così Corte cost., sent. n. 2/1956. Nuvolone (1956), p. 441.

ne pubblico, alla sicurezza dei cittadini, alla loro incolumità e alla tutela della proprietà; cura l'osservanza delle leggi e dei regolamenti generali e speciali dello Stato, delle province e dei comuni, nonché delle ordinanze delle autorità; presta soccorso nel caso di pubblici e privati infortuni".

Nella prospettiva della prevenzione, il compito dello Stato "non è tanto (o meglio, non è solo) garantire il diritto alla sicurezza personale dei singoli individui, quanto la complessiva sicurezza dei diritti dei cittadini e dei beni giuridici loro sottesi, in un contesto sociale complesso"[9]. Questa duplice dimensione[10] di sicurezza trova efficace sintesi all'art. 2 della Costituzione che, nel riconoscere e garantire i diritti inviolabili dell'uomo, richiede tuttavia l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale. Accanto alle "libertà c.d. negative", espressione della concezione liberale classica preoccupata di tutelare la persona da indebite limitazioni delle pubbliche autorità, consentite a fronte della duplice riserva[11] di legge e giurisdizione (ad esempio gli artt. 13, 14 e 15 Cost.), con l'affermazione del costituzionalismo liberaldemocratico, allo Stato è consentito intervenire a tutela di esigenze collettive connesse alle "libertà c.d. positive", avuto riguardo ai diritti sociali ed economici (ad esempio, gli artt. 32, 41, 42 Cost.)[12]: trovano così composizione esigenze individuali e collettive di tutela ed in questa prospettiva, l'interpretazione estesa della nozione di sicurezza consente di cogliere lo specifico profilo economico-finanziario nella cui cornice sono esercitabili le libertà economiche[13].

La polizia di sicurezza[14] si concreta nelle varie attività finalizzate al riscontro e alla ricerca di situazioni "oggettive" di pericolo o di inizio di attività criminose. Essa si distingue pertanto dalla polizia amministrativa[15] che, con il trasferimento delle funzioni amministrative dallo Stato alle regioni e agli enti locali, ha perso autonomia per divenire strumentale rispetto alle funzioni di amministrazione attiva[16]. Un'ultima distinzione corre tra la polizia di sicurezza e la polizia giudiziaria. Con la prima si identifica tutta l'attività di tutela dell'ordine e della sicurezza pubblica di competenza dell'autorità amministrativa. Essa ha carattere preventivo in quanto è tesa ad impedire qualunque violazione dell'ordine sociale e si differenzia dalla polizia giudiziaria le cui funzioni sono esercitabili, alle dipendenze e sotto la direzione dell'autorità giudiziaria, all'emergere degli indizi di un fatto penalmente rilevante.

Se la logica del bilanciamento giustifica la compressione dell'interesse individualmente tutelato, secondo il metodo della valutazione in concreto nell'applicazione delle scriminanti, nella più ampia accezione di sicurezza, un limite implicito ed ordinario all'esercizio di alcuni diritti è connesso alle attività di prevenzione integranti l'attività di polizia.

Al di fuori dei casi che rendono necessaria le riserve di legge e giurisdizione, le potestà di

[9] Si veda Giupponi (2007), per il quale questa visione "mette al centro non tanto l'individuo inteso come essere a sé stante, isolato dal contesto sociale di riferimento, ma la persona umana nelle sue relazioni sociali, centro di imputazione di diritti e di doveri [a garanzia] non solo della "*sicurezza da*" potenziali intrusioni nell'ambito di sfere individuali di libertà, ma anche della "*sicurezza di*" poter esprimere in pieno la propria personalità, attraverso il patrimonio costituzionale dei diritti e nell'ambito del (e non prescindendo dal) contesto sociale di riferimento". In senso conforme, per il Cons. Stato, Sez. VI, sent. 16.01.2006, n. 85, "le libertà individuali, nello Stato sociale, vanno coniugate all'unisono con l'interesse della collettività e subiscono delle compressioni in talune modalità di esercizio, per renderle compatibili con le libertà pari ordinate di altri". Leone (2006), p. 3479.

[10] Tale ambivalenza si ritrova a livello internazionale, ad esempio nella CEDU e nei diritti fondamentali, preservati rispetto all'ingerenza dello Stato, a meno che l'intervento pubblico non rappresenti una misura necessaria, in una società democratica, alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

[11] Per l'approfondimento si rinvia ad Angiolini (1992).

[12] L'impostazione solidaristica consente di cogliere clausole costituzionali di socialità per il richiamo ai doveri di solidarietà (art. 2), alla dimensione sostanziale dell'uguaglianza (art. 3), alla libertà dell'iniziativa economica privata che "non può svolgersi in contrasto con l'utilità sociale" (art. 41), alla "funzione sociale" della proprietà (art. 42) nonché al dovere di concorrere alla spesa pubblica in ragione della propria capacità contributiva (art. 53).

[13] Sulla sicurezza economico finanziaria quale autonomo bene giuridico, a garanzia dello sviluppo economico e delle condizioni sociali e finanziarie della comunità nazionale, si rinvia a Ricozzi C. e di Paolo N. (2003), p. 1485.

[14] Per l'approfondimento si rinvia a Corso (1996) p. 319.

[15] Sul tema si veda Nova (1996), p. 314.

[16] Avviato dall'art. 9 del D.P.R. 24.7.1977, n. 616, tale trasferimento si è concluso con l'art. 161 del D.Lgs. 31.03.1998, n. 112. La ripartizione delle attribuzioni relativa alle funzioni di polizia è fondata sulla distinzione tra le competenze attinenti alla pubblica sicurezza, riservate in via esclusiva allo Stato *ex* art. 4 del D.P.R. 616/1977, e le altre enucleate dall'ampia categoria della polizia amministrativa e trasferite alle regioni come funzioni accessorie ai settori materiali loro attribuiti. Mentre le prime […] riguardano le misure preventive e repressive dirette al mantenimento dell'ordine pubblico e, pertanto, si riferiscono alle attività tradizionalmente ricomprese nei concetti di polizia giudiziaria e di quella di pubblica sicurezza (in senso stretto), le altre invece concernono le attività di prevenzione o di repressione dirette a evitare danni o pregiudizi che possono essere arrecati alle persone o alle cose nello svolgimento di attività ricomprese nelle materie sulle quali si esercitano le competenze regionali […], senza che ne risultino lesi o messi in pericolo i beni o gli interessi tutelati in nome dell'ordine pubblico". Così Corte cost., sent. n. 218/1988. Travi (1988), p. 830. Si veda anche n. 162/1990. Corso (1990), p. 1006.

polizia operano come limite esterno[17] ed in forme differenziate perché esistono differenti poteri di polizia. Ai nostri fini prenderemo in considerazione l'utilizzo delle banche dati nonché il bilanciamento tra il diritto alla protezione dei dati personali, da ultimo espressamente previsto all'art. 8 della Carta dei diritti fondamentali dell'Unione europea, con l'interesse generale alle attività di prevenzione, indagine, accertamento e perseguimento di reati, come disciplinato dal D.Lgs. 18.05.2018 n. 51, di attuazione della Direttiva (UE) 2016/680 del 27 aprile 2016, sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali[18].

Poiché l'art. 1, secondo comma, circoscrive l'ambito di applicazione del D.Lgs. 51/2018, tra l'altro, "al trattamento interamente o parzialmente automatizzato di dati personali delle persone fisiche" svolto con tali finalità, il profilo saliente è segnalare l'incidenza delle nuove tecnologie sulla funzione informativa dell'operatore di polizia giudiziaria, la cui attività è adesso agevolata dalla consultazione delle banche dati e, soprattutto, dalla loro interoperabilità.

Tale analisi sarà declinata con riferimento all'adempimento obbligazione tributaria, che sorge in presenza di un fatto espressivo di capacità contributiva ed in base alla quale, ai sensi dell'art. 53 della Costituzione, ciascuno è tenuto a concorrere alla spesa pubblica quale adempimento del dovere di solidarietà economica sancito al precedente art. 2[19]: tali riferimenti consentono l'aggancio costituzionale del bene giuridico tutelato, in via diretta o mediata, dalle incriminazioni contenute nel D.Lgs. 10.03.2000, n. 74[20].

3. Il filo conduttore tra analisi economica del diritto, politica criminale e nuove tecnologie.

Tra le discipline aventi ad oggetto le possibili interrelazioni tra il diritto e l'economia[21], l'analisi economica del diritto studia le norme giuridiche in relazione alla loro efficacia, con particolare riferimento, tra l'altro, alla loro capacità concreta di disincentivare determinati comportamenti. Poiché considera tali norme come strumento di governo per raggiungere determinati obiettivi, il metodo dell'analisi economica applicato alle scelte di politica criminale consentirebbe, ad avviso di alcuni, di ripensare razionalmente il sistema sanzionatorio[22].

[17] L'impostazione solidaristica consente di cogliere clausole costituzionali di socialità nell'esercizio di alcuni diritti, i quali possono soffrire limiti esterni, per il bilanciamento con altre situazioni meritevoli, ed interni per il divieto dell'abuso del diritto cioè del suo esercizio con finalità diverse e finanche in contrasto con quelle di attribuzione.

[18] Nel preambolo della Direttiva risulta che "le attività svolte dalla polizia o da altre autorità preposte all'applicazione della legge vertono principalmente sulla prevenzione, l'indagine, l'accertamento o il perseguimento di reati, comprese le attività di polizia condotte senza previa conoscenza della rilevanza penale di un fatto. Tali attività […] comprendono anche il mantenimento dell'ordine pubblico quale compito conferito alla polizia […] ove necessario per la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica e agli interessi fondamentali della società tutelati dalla legge che possono dar luogo a reati […]" (n. 12) e che, per le accennate finalità , "è necessario che le autorità competenti trattino i dati personali raccolti a fini di prevenzione, indagine, accertamento o perseguimento di specifici reati al di là di tale contesto per sviluppare conoscenze delle attività criminali e mettere in collegamento i diversi reati accertati" (n. 27).

[19] Premesso che un fatto espressivo di capacità contributiva è un fatto che esprime forza economica, "collegando i tributi alla capacità contributiva [l'art. 53 Cost.] deve essere visto, dal lato del legislatore, come una norma che ne vincola e limita il potere; dal lato dei contribuenti, come una norma di garanzia". Così Tesauro (2011), p. 65. Nella giurisprudenza costituzionale è stato individuato il nesso tra gli art. 2 e 53 della Carta fondamentale. Si veda Corte cost., sent. n. 51/1992. Falsitta (1992) p. 566. Di tale rapporto, tuttavia, si è progressivamente accentuato il profilo verticale della solidarietà economica, quella del singolo verso la pubblica amministrazione, piuttosto che orizzontale, tra e verso i membri della collettività. Sul tema Corte cost., sent. n. 351/2000.

[20] Sul bene giuridico tutelato nei reati tributari si rinvia a Musco (2007), p. 1044.

[21] Sui diversi profili si veda Sorbello (2016b), p. 1918.

[22] Invero, l'utilità dello strumento è stata finora circoscritta ai reati economici caratterizzati dal "modello del delinquente calcolatore" e non troverebbe applicazione alla delinquenza per motivazione non lucrativa. Così Mantovani (2006), p. 1173. L'applicabilità del metodo, tuttavia, appare superare l'ambito (oggettivo) del "diritto penale dell'economia" per volgere al profilo (soggettivo) dell'agente razionale che rimane tale anche se non persegue un vantaggio, ma vuole soltanto allontanare o attenuare uno svantaggio, orientando le sue scelte in relazione a tutte le conseguenze negative. Così Sorbello (2016 b), p. 1934. Le origini del metodo dell'analisi economica del diritto si fanno risalire a Cesare Beccaria il quale, nel saggio sul "Tentativo analitico sui contrabbandi" pubblicato nel 1764, si pose l'obiettivo di fornire al costruttore di tariffe gli strumenti per determinare il giusto dazio da applicare alle merci per dissuadere il contrabbando. A tal fine, premesso che alla scoperta dell'introduzione illegale di merce consegue la perdita della merce stessa, mentre il rischio per lo Stato è legato proporzionalmente al valore del tributo, quello del contrabbandiere lo è invece al valore delle mercanzia: se il tributo ha un valore maggiore rispetto a quello della merce, sarà lo Stato ad assumere il rischio più elevato in quanto per l'importatore sarà comunque più conveniente introdurre illegalmente la merce. Inoltre, il rischio per il contrabbandiere cresce in relazione al numero di controllori e diminuisce, invece, in relazione ai volumi importati perché legato sia alla probabilità di essere scoperti che al valore delle merce introdotta illegalmente. Tra i primi scritti nella letteratura americana, alla quale si deve lo sviluppo del metodo e l'applicazione nelle diverse branche dell'ordinamento, si segnalano Coase (1960), Calabresi (1961) e Becker (1968).

Nella prospettiva di una generalizzazione, nei limiti del possibile, di questo metodo, occorre verificare l'utilità scientifica di una teoria del reato economicamente fondata[23] tenuto conto che, accanto agli istituti "moderni" del diritto penale (ad esempio responsabilità degli enti e confisca per equivalente), l'analisi economica del diritto fornisce indicazioni utili anche nell'affrontare le categorie tradizionali, con l'obiettivo di intervenire sui più rilevanti problemi normativi. A garanzia della razionalità (e quindi efficacia[24]) del sistema penale, infatti, la politica criminale deve intervenire sulle probabilità di essere scoperti, di giungere all'irrogazione della sanzione e di annullare qualsivoglia utilità conseguita dalla violazione del precetto: poiché l'analisi economica valorizza il collegamento fra strategie di politica criminale e valutazione, in capo al potenziale trasgressore, dei costi e benefici connessi alla scelta di violare la regola, la propensione del soggetto razionale alla violazione è inversamente proporzionale alle probabilità sopra indicate.

Le successive riflessioni considereranno soltanto il primo dei problemi normativi.

Poiché l'aumentare le probabilità di scoprire le violazioni incontra limiti strutturali, che non consentono di potenziare illimitatamente le autorità pubbliche di controllo, occorre prestare attenzione alla *partnership* pubblico-privato[25] basata sul principio della collaborazione attiva in funzione preventiva di determinati reati, come avviene da tempo in materia antiriciclaggio[26], ma non solo[27]. Una simile collaborazione è infatti stimolata dalle conseguenze negative, ad esempio le sanzioni per la violazione di obblighi integranti illeciti omissivi propri[28] nonché, a determinate condizioni, l'equivalenza normativa di cui all'art. 40 cpv c.p.[29]. Nonostante l'avvertenza che l'accrescimento della pluralità dei soggetti e dei tipi del controllo può indurre fenomeni di sovrapposizione delle attività[30], l'attenzione alle conseguenze negative minacciate per la mancata collaborazione consente però di generalizzare una posizione di contrasto d'interesse idonea ad orientare il soggetto obbligato verso la collaborazione.

Se, in estrema sintesi, questo problema normativo investe l'acquisizione della notizia di reato, la nostra attenzione non è immediatamente rivolta alla disciplina della singola funzione (informativa) di polizia giudiziaria[31], la prima tra quelle disciplinate dall'art. 55 c.p.p., che potrebbe risultare poco interessante per il diritto penale. Al contrario, questo momento è particolarmente significativo per il diritto penale nella prospettiva della politica criminale e quindi di scopo, che è quello di limitare le offese all'ordinamento penale, anche ricorrendo a strumenti non di natura penale né esclusivamente di tipo sanzionatorio, qualunque sia la loro natura.

Il filo conduttore che lega analisi economica del diritto e politica criminale, nuove tecnologie e diritto (e procedura) penale può adesso risultare più chiaro perché un'ulteriore soluzione è offerta dalle nuove tecnologie, in particolare dal trattamento[32] automatizzato di dati (anche personali) "a fini di prevenzione, indagine, accertamento e perseguimento di reati" come disciplinato dal d.lgs. 51/2018, di attuazione della citata Direttiva 2016/680.

Alle opportunità offerte dalle nuove tecnologie si affianca però il rischio di assumere de-

[23] Così Paliero (2005), p. 1396.

[24] La valutazione sull'efficacia di una regola si risolve in un giudizio di funzionalità o, in termini weberiani, di "razionalità rispetto allo scopo", subordinato alla verifica dell'idoneità delle soluzioni adottate a conseguire gli obiettivi attesi: una legge è razionale se funziona ed in questo caso è anche utile. Questa progressione razionalità-funzionalità-utilità investe il concetto di effettività ed è legata all'idea di scopo, che esige l'adeguamento del mezzo al fine, caratterizzante la politica criminale.

[25] Per Centonze (2011), p. 1759, "il trasferimento ai privati di compiti di prevenzione rappresenta, d'altra parte, un esempio assai emblematico delle ormai ricorrenti politiche di delega ai privati di compiti di sorveglianza di fatti illeciti.

[26] Il riferimento è al principio di collaborazione attiva sul quale è fondato l'obbligo di segnalare le operazioni sospette di riciclaggio ai sensi dell'art. 35 del d.lgs. 21.11.2007, n. 231.

[27] La prospettiva è rilevante anche in materia di abusi di mercato, con le segnalazioni di operazioni sospette *ex* art. 187-*nonies* del d.lgs. 58/1998; contrasto alla corruzione avuto riguardo alla segnalazione degli illeciti (c.d. *whistleblowing*) introdotta originariamente all'art. 54-*bis* del d.lgs. 165/2001; sicurezza sul lavoro, per la segnalazione da parte del rappresentante dei lavoratori per la sicurezza e la prevenzione ai sensi dell'art. 50, primo comma, lett. n), del d.lgs. 81/2008.

[28] Il riferimento è, ad esempio, all'inosservanza dell'obbligo della segnalazione di operazioni sospette sanzionata in via amministrativa, salvo che il fatto non costituisca reato, dall'art. 58 del d.lgs. 231/2007.

[29] Si veda Sorbello (2015), p. 442. Conforme, Cass. pen., Sez. III, sent. 08.03.2016, n. 9472.

[30] Così Flick (2015), p. 7.

[31] Sul tema si rinvia ad Aprati (2010).

[32] Ai sensi dell'art. 2 (Definizioni) del d.lgs. 51/2018 deve intendersi per "[…] b) *trattamento*: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione; [nonché per] e) *profilazione*: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti […] la situazione economica […]".

cisioni basate unicamente su un trattamento automatizzato (compresa la profilazione) che producono effetti negativi nei confronti dell'interessato: si tratta di un'insuperabile linea rossa, garantita teoricamente dal divieto posto dall'art. 11 della citata Direttiva[33] e che porta con sé le implicazioni etiche dell'automazione relative alle conseguenze discriminatorie. Questi aspetti, che superano gli orizzonti delle nostre riflessioni, costituiscono un monito nel ricordare che "il trattamento dei dati personali dovrebbe essere al servizio dell'uomo" 34 ed ispirare un impiego delle nuove tecnologie "nella direzione di un nuovo umanesimo digitale"[35].

4. Analisi del rischio di evasione, interoperabilità delle banche dati ed utilizzo delle informazioni antiriciclaggio.

Se la sanzione rappresenta lo strumento predisposto dall'ordinamento per assicurare l'osservanza del precetto, sul piano tributario essa riveste importanza ulteriore perché alla funzione anzidetta si affianca quella di garantire il gettito erariale.

Ad una ricognizione del sistema sanzionatorio tributario negli ultimi cinquant'anni, tuttavia, emergerebbe un complesso normativo in continuo divenire, nel quale la necessità del contingente ha giustificato il susseguirsi di interventi spesso di segno opposto, apparentemente ispirati da logiche di cassa nel breve periodo. Tenuto poi conto che l'effettività del precetto tributario passa anche per la conseguente (certa) sanzione per la loro inosservanza, il ciclico verificarsi di variabili (i c.d. condoni) che intaccano questa regolarità crea un corto circuito dell'efficacia generalpreventiva del sistema, in ragione dell'affidamento del contribuente nella prossima sanatoria[36]. In un sistema fiscale basato sull'adempimento spontaneo dell'obbligazione tributaria, infatti, la capacità della norma di orientare il comportamento secondo le attese è subordinata al messaggio che l'illecito risparmio d'imposta non solo non è mai conveniente, ma risulta anzi costoso: "un'efficace politica antievasione si basa sulla capacità di deterrenza dell'amministrazione piuttosto che su un inattuabile e costoso controllo della massa dei contribuenti"[37].

Tenuto conto che la scelta di evadere dipende in maniera critica dalla probabilità percepita di subire un accertamento, una svolta epocale si ebbe con l'incremento della capacità di controllo dell'amministrazione finanziaria a seguito dell'entrata in vigore della legge 30.12.1991, n. 413.

In particolare, ai sensi del quarto comma dell'art. 20 "con decreto del Ministro del tesoro, di concerto con i Ministri dell'interno e delle finanze, da emanare entro sessanta giorni dalla data di entrata in vigore della presente legge, sono stabilite, con il massimo di elementi di ri-

[33] Per il considerando n. 38 della Direttiva "l'interessato dovrebbe avere il diritto di non essere oggetto di una decisione che valuta aspetti personali che lo concernono basata esclusivamente su un trattamento automatizzato e che produca effetti giuridici negativi nei suoi confronti o incida significativamente sulla sua persona. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, compresi il rilascio di specifiche informazioni all'interessato e il diritto di ottenere l'intervento umano, in particolare di esprimere la propria opinione, di ottenere una spiegazione della decisione raggiunta dopo tale valutazione e di impugnare la decisione. La profilazione che porti alla discriminazione di persone fisiche sulla base di dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali dovrebbe essere vietata […]". Tale divieto è stato attuato dall'art. 8 del d.lgs. 51/2018.

[34] Così il considerando n. 4 del Regolamento (UE) 2016/679 del 27.04.2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, il quale precisa però che "il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità". Ai sensi dell'art. 2, secondo comma, lett. d), il Regolamento non si applica ai trattamenti di dati personali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

[35] In questi termini Soro (2017), pag. 8 ss., per il quale "dall'esattezza dei dati utilizzati e dalla logica del trattamento alla base della configurazione degli algoritmi dipende l'intelligenza delle loro scelte. […] Le possibili implicazioni, sul piano sociale, sono tutt'altro che marginali. Gli algoritmi non sono neutri sillogismi di calcolo, ma opinioni umane strutturate in forma matematica che, come tali, riflettono, in misura più o meno rilevante, le precomprensioni di chi li progetta, rischiando di volgere la discriminazione algoritmica in discriminazione sociale. Rispetto a questi rischi, risultano importanti le garanzie sancite dal nuovo quadro giuridico in ordine ai processi decisionali automatizzati, assicurandone […], almeno in ultima istanza, il filtro dell'uomo, per contrastare la delega incondizionata al cieco determinismo della tecnologia. […] Al di là del quasi ancestrale timore di un uomo vittima delle sue creazioni, emerge quindi il bisogno di fondare basi etiche e giuridiche solide per uno sviluppo davvero sostenibile, perché la tecnologia deve poter servire e integrare, senza sostituire, l'intelligenza umana".

[36] Si vedano Falsitta (2003), p. 794, e Martini (2010) p. 69 ss., per il quale "nessun sistema repressivo penale ha dovuto sopportare tanto quanto il c.d. diritto penale tributario, che la propria efficacia repressiva fosse condizionata dal succedersi nel corso degli anni, di provvedimenti di clemenza [...] Il contribuente ha finito così per acquisire una sorta di consolidata consapevolezza della scarsa effettività della minaccia formulata dal legislatore con la prospettazione della fattispecie incriminatrice, sapendo di poter contare su una sorta di impunità".

[37] "Da un punto di vista teorico, si evade perché esiste una convenienza economica. [...] se il beneficio derivante dall'evasione supera il costo atteso associato alla possibilità di un accertamento". Così Ministro dell'economia e delle finanze (2007), par. 16.

servatezza, la destinazione e le modalità delle comunicazioni da parte delle aziende ed istituti di credito e dell'Amministrazione postale nonché delle società fiduciarie e di ogni altro intermediario finanziario dei dati identificativi, compreso il codice fiscale, di ogni soggetto che intrattenga con loro rapporti di conto o deposito o che comunque possa disporre del medesimo, nonché i criteri per le relative utilizzazioni": nonostante il termine di sessanta giorni, il provvedimento attuativo è stato adottato solo con D.M. 04.08.2000 n. 269, istitutivo dell'anagrafe dei rapporti di conto e deposito ed attualmente in vigore e di interesse per quanto riguarda l'indicazione dei soggetti, elencati all'art. 4, abilitati alla consultazione[38].

Nell'avviare il progressivo smantellamento del segreto bancario[39], la nuova disciplina mise a disposizione lo strumento delle indagini finanziarie reso ancor più incisivo da provvedimenti successivamente adottati, tra i quali l'archivio dei rapporti con gli operatori finanziari, sostitutivo dell'anagrafe dei conti e dei depositi, in grado di consentire agli organi di controllo l'automatica individuazione degli intermediari in effettivo rapporto con il contribuente nella complessiva platea dei potenziali destinatari delle richieste di accesso alla documentazione finanziaria[40].

L'archivio dei rapporti finanziari è regolato dall'art. 7, sesto comma, del D.P.R. 29.09.1973, n. 605, recante disposizioni relative all'anagrafe tributaria e al codice fiscale dei contribuenti, che regolamenta i flussi di comunicazione indirizzati all'Amministrazione finanziaria. Si tratta di una banca dati che costituisce una speciale sezione dell'Anagrafe Tributaria, implementata attraverso le comunicazioni periodiche degli intermediari, finalizzata a contenere tutte le informazioni che possono essere acquisite dagli organi di controllo fiscale, attraverso l'esercizio dei poteri di indagine finanziaria, nel rispetto della normativa in materia di riservatezza e protezione dei dati personali.

Sotto il profilo temporale, l'archivio accoglie le informazioni sui rapporti in essere e le operazioni extraconto, effettuate a partire dal 1° gennaio 2005, ed è aggiornato ogni mese con riferimento alle operazioni del mese precedente. In sintesi, esso contiene attualmente:

- per ciascun rapporto segnalato, informazioni sulla tipologia sulle date di accensione, variazione ed eventuale cessazione, sui dati identificativi delle persone fisiche o giuridiche titolari, contitolari o collegate ai rapporti medesimi, nonché la tipologia di collegamento;
- per le operazioni finanziarie effettuate al di fuori di un rapporto continuativo, i dati identificativi dei soggetti che le effettuano, per conto proprio o a nome di terzi.

Rispetto alla disciplina originariamente introdotta dall'art. 20 della legge 413/1991, l'art. 7 del D.P.R. 605/1973 è stato modificato più volte. Tra le disposizioni più rilevanti si segnala:

- la legge 311/2004, con l'estensione degli obblighi di rilevazione rispetto, da un lato,

[38] Sul punto Tridico (2017) ha evidenziato che "nonostante fin dal 1991 fosse prevista, previa adozione di un d.m. da emanarsi entro sessanta giorni, l'Anagrafe dei rapporti di conto e di deposito, sia pure riguardante la raccolta dei soli dati anagrafici, il decreto è stato adottato dopo dieci anni e, peraltro, non ha mai trovato concreta attuazione. L'Anagrafe dei rapporti finanziari, in concreto, è divenuta effettivamente operativa ed accessibile da tutti i soggetti legittimati solo nel 2009. Se per il suo impianto definitivo, quindi, sono emersi ritardi particolarmente importanti, ben più grave è la situazione riscontrata relativa al suo concreto ed effettivo utilizzo per la lotta all'evasione, per il quale deve rilevarsi una grave inadempienza dell'Agenzia, che non ha mai elaborato le previste liste selettive né, successivamente, le analisi del rischio evasione e, di conseguenza, non ha potuto riferire alle Camere sui risultati nella lotta all'evasione derivanti dall'utilizzo dell'Anagrafe dei rapporti finanziari. È stato quindi, ad oggi, del tutto pretermesso di dare attuazione a un chiaro disposto normativo". Le disposizioni per le analisi di rischio di evasione sono state emanate con il provvedimento del Direttore dell'Agenzia delle Entrate n. 197357 del 31.08.2018.

[39] "Con il termine di segreto bancario si denota un dovere di riserbo cui sono tradizionalmente tenute le imprese bancarie in relazione alle operazioni, ai conti e alle posizioni concernenti gli utenti dei servizi da esse erogati. A tale dovere, tuttavia, non corrisponde nei singoli clienti delle banche una posizione giuridica soggettiva costituzionalmente protetta, né, men che meno, un diritto della personalità, poiché la sfera di riservatezza […] è direttamente strumentale all'obiettivo della sicurezza e del buon andamento dei traffici commerciali. In ragione di ciò, il se, il quanto e il come della tutela del segreto bancario sono lasciati alla scelta discrezionale del legislatore ordinario, il quale, in tale valutazione, è tenuto a un non irragionevole apprezzamento dei fini di utilità e di giustizia sociale che gli artt. 41, secondo comma, e 42, secondo comma, della Costituzione prevedono […] resta fermo, comunque, che le scelte discrezionali del legislatore, ove si orientino a favore della tutela del segreto bancario, non possono spingersi fino al punto di fare di questo ultimo un ostacolo all'adempimento di doveri inderogabili di solidarietà, primo fra tutti quello di concorrere alle spese pubbliche in ragione della propria capacità contributiva (art. 53 della Costituzione), ovvero fino al punto di farne derivare il benché minimo intralcio all'attuazione di esigenze costituzionali primarie, come quelle connesse all'Amministrazione della Giustizia e, in particolare, alla persecuzione dei reati". Così Corte cost., sent. n. 51/1992.

[40] Si veda Comando Generale della Guardia di Finanza (2018), p. 215 ss., dalla quale è tratta la presente sintesi sulla disciplina dell'archivio dei rapporti finanziari.

a tutti gli intermediari interessati[41] e, dall'altro, a qualsiasi rapporto[42] intrattenuto e qualsiasi operazione eseguita in favore dei propri clienti;

- il D.L. 223/2006, con l'introduzione, accanto alla rilevazione dei dati, dell'obbligo di comunicazione all'Anagrafe tributaria. Quest'ultimo decreto ha fissato le regole generali per l'accesso all'archivio, prevedendone la consultazione per finalità tassative[43], ulteriori rispetto alle indagini in campo tributario, poi progressivamente ampliate[44];
- il d.lgs. 231/2007, in materia antiriciclaggio, con la previsione dell'obbligo di comunicare le informazioni relative a "qualsiasi operazione" di natura finanziaria posta in essere dai propri clienti, unitamente ai dati identificativi e al codice fiscale dei soggetti che intrattengono qualsiasi rapporto o effettuano operazioni al di fuori di un rapporto continuativo per conto proprio o a nome di terzi.

Fino al 2011 le indagini finanziarie erano "serventi" rispetto ai controlli tributari perché occorreva prima individuare la posizione del contribuente da controllare e soltanto in seguito poteva consultarsi l'archivio dei rapporti finanziari secondo le ordinarie procedure previste dagli artt. 32, primo comma, numero 7), del D.P.R. 600/1973, n. 600, e 51, secondo comma, numero 7), del D.P.R. 633/1972.

L'ulteriore potenziamento della disciplina si è avuta con l'art. 11 del D.L. 16.12.2011, n. 201 (c.d. Decreto "Salva Italia"), convertito, con modificazioni, dalla legge 22.12.2011, n. 214. Nell'ottica di rendere più efficace l'azione di contrasto all'evasione fiscale, infatti, a partire dal 1° gennaio 2012, gli operatori finanziari sono obbligati a comunicare periodicamente all'anagrafe tributaria:

- le movimentazioni che hanno interessato i rapporti continuativi, la cui esistenza era già oggetto di comunicazione, ed ogni altra informazione riferita a questi rapporti necessaria ai fini dei controlli fiscali;
- l'importo delle operazioni extra-conto (richiesta per contanti di assegni e bonifici, il cambio di valuta e assegni, ecc.), per le quali era già da tempo prevista la trasmissione dei dati anagrafici dei titolari e dei soggetti che le effettuano.

La *ratio* di tali norme, come evidenziato nella relazione di accompagnamento al decreto, è stata permettere di acquisire la movimentazione dei dati finanziari a cadenza periodica[45] e non

[41] La platea dei destinatari è stata ampliata dal D.L. 06.07.2011, n. 98, convertito, con modificazioni, dalla legge 15.07.2011, n. 111, con l'inserimento degli intermediari assicurativi, limitatamente alle attività finanziarie esercitate.

[42] Sono incluse anche le informazioni sulle disponibilità finanziarie rimpatriate con l'adesione alla procedura di cui all'art. 13-*bis* del D.L. 01.07.2009, n. 78, convertito, con modificazioni, dalla legge 03.08.2009, n. 102 (c.d. "scudo fiscale *ter*). Con il provvedimento del 9 agosto 2013, l'Agenzia ha infatti precisato "poiché tutti i conti perverranno in maniera indistinta, appare coerente che nel flusso vengano inclusi anche i conti scudati".

[43] Ai sensi dell'art. 7, undicesimo comma, del D.P.R. 603/1975, le comunicazioni sono utilizzate:
- per le richieste di cui all'art 32, primo comma, numero 7), del D.P.R. 29.09.1973, n. 600, e all'art. 51, secondo comma, numero 7), del D.P.R. 26.10.1972, n. 633, in materia di accertamento delle imposte dirette e sul valore aggiunto;
- per le attività connesse alla riscossione mediante ruolo;
- dai soggetti di cui all'art. 4, comma 2, lettere a), b), c) ed e), del D.M. 04.08. 2000, n. 269, ai fini degli accertamenti finalizzati alla ricerca e all'acquisizione della prova e delle fonti di prova nel corso di un procedimento penale, sia ai fini delle indagini preliminari e dell'esercizio delle funzioni previste dall'art. 371-*bis* c.p.p., sia nelle fasi processuali successive, ovvero degli accertamenti di carattere patrimoniale per le finalità di prevenzione previste da specifiche disposizioni di legge e per l'applicazione delle misure di prevenzione.

[44] L'accesso all'archivio dei rapporti finanziari è stato altresì previsto da:
- l'art. 187-*octies*, quarto comma, lett. e-*bis*), del D.Lgs. 24.02.1998, n. 58, con riferimento ai poteri della CONSOB in materia di abusi di mercato;
- gli artt. 1, quinto comma 5, lett. b), del D.L. 03.10.2006, n. 262/2006 e 15, comma 8-*duodecies*, del D.L. 01.07.2009, n. 78, per quanto riguarda i compiti amministrativi e tributari dell'Agenzia delle dogane e dei monopoli;
- l'art. 8 (ora 9) del D.Lgs. 21.11.2007, n. 231, nell'esercizio dei poteri di polizia valutaria in materia antiriciclaggio;
- l'art. 83, comma 28-*sexies*, del D.L. 25.06.2008, n. 112, per la consultazione da parte dei Comuni e dei soggetti da essi autorizzati alla riscossione dei tributi;
- l'art. 25 del D.L. 22.06.2012, n. 83, estendendo i poteri di polizia valutaria nel controllo sulle erogazioni pubbliche;
- l'art. 19 del D.L. 12.09.2014, n. 132, che ha aggiunto l'art. 492-*bis* c.p.c.: previa autorizzazione del Tribunale, al creditore è garantita la fruibilità delle informazioni ivi contenute per una migliore efficienza del processo esecutivo;
- l'art. 3 del D.L. 22.10.2016, n. 193, che ha potenziato la riscossione, consentendo all'Agenzia delle entrate e all'ente strumentale Agenzia delle entrate-Riscossione di utilizzare l'archivio anche ai fini delle funzioni relative alla riscossione.

[45] Le disposizioni attuative dell'art. 11, commi secondo e terzo, del D.L. 201/2011 sono state adottate dal Direttore dell'Agenzia delle Entrate con il provvedimento n. 37561 del 25.03.2013, in base al quale devono essere inviate con cadenza annuale. In particolare, il provvedimento direttoriale precisa che debbano essere comunicati, tra l'altro:
- i dati relativi al saldo iniziale (1° gennaio) e finale (31 dicembre) del rapporto, relativi all'anno di riferimento della comunicazione;

soltanto ad attività di controllo già avviata, fornendo così all'Amministrazione finanziaria uno strumento di straordinaria efficacia nel contrasto all'evasione fiscale.

In particolare, l'art. 11, quarto comma, del D.L. 201/2001 ha previsto l'utilizzabilità di tutte le informazioni confluite nell'archivio ai sensi dell'art. 7, undicesimo comma, del D.P.R. 605/1973. Inoltre, le informazioni relative alle comunicazioni integrative (afferenti ai saldi dei rapporti) sarebbero dovute essere utilizzate[46] dall'Agenzia delle Entrate per l'elaborazione di specifiche liste selettive dei contribuenti a maggior rischio di evasione. Tale elaborazione, da sviluppare con procedure centralizzate e secondo criteri individuati con apposito provvedimento dell'Agenzia delle Entrate, allo stato attuale mai emanato, non è mai avvenuta anche a seguito delle disposizioni introdotte dall'art. 1, comma 314, della legge 23.12.2014, n. 190 (legge di stabilità 2015) che ha riscritto il citato quarto comma dell'art. 11, modificando così le norme sull'utilizzo delle informazioni periodicamente comunicate all'Archivio dei rapporti.

In estrema sintesi, mentre prima della legge di stabilità 2015 tutte le informazioni presenti nell'anagrafe tributaria[47] sarebbero dovute essere utilizzate dall'Agenzia delle Entrate per la formazione di apposite liste selettive di controllo, con la successiva modifica dell'art. 11, quarto comma, è stato previsto che le medesime informazioni[48] siano "utilizzate dall'Agenzia delle entrate per le analisi del rischio di evasione", senza rinvio ad alcun provvedimento attuativo, secondo criteri definiti annualmente dall'Amministrazione finanziaria. Le disposizioni attuative dell'art. 11, quarto comma, del D.L. 201/2011 sono state adottate con il provvedimento del Direttore dell'Agenzia delle Entrate n. 197357 del 31.08.2018, che ha previsto una procedura sperimentale per l'analisi del rischio di evasione[49]. Tale fase, relativa alla posizione fiscale di società di persone e società di capitali, consiste nell'utilizzo integrato delle informazioni comunicate dagli operatori all'archivio dei rapporti finanziari e degli altri elementi presenti in anagrafe tributaria e consentirà di estrapolare le società per le quali, pur risultando sui conti correnti movimenti in accredito, per l'anno di imposta 2016, la dichiarazione ai fini delle imposte dirette ed ai fini IVA è stata omessa o presentata priva di dati contabili significativi[50].

L'ultimo intervento normativo che ha ulteriormente valorizzato il ricorso all'archivio dei rapporti finanziari, nonché l'incrocio delle informazioni complessivamente disponibili in capo all'amministrazione finanziaria, è rappresentato dal D.L. 23.10.2018, n. 119[51] recante disposizioni urgenti in materia fiscale e finanziaria, che ha ampliato la possibilità di effettuare analisi di rischio consentendo così indagini economico-finanziarie ancor più mirate[52]. Intervenendo

- per i rapporti accesi nel corso dell'anno, il saldo alla data di apertura;
- per i rapporti chiusi nel corso dell'anno, il saldo antecedente alla data di chiusura;
- i dati relativi agli importi totali delle movimentazioni, distinte tra dare ed avere, per ogni tipologia di rapporto, conteggiati su base annua.

Per alcune tipologie di rapporto sono richieste ulteriori informazioni in particolare, in ordine:

- alle cassette di sicurezza, il numero totale degli accessi avvenuto per anno, nonché i massimali previsti per eventuali assicurazioni accese sulle stesse;
- alle operazioni extra-conto, oltre all'ammontare delle operazioni, il numero delle operazioni effettuate nell'anno;
- alle carte di credito, oltre all'utilizzo del plafond di spesa a inizio e fine anno, il totale degli acquisti effettuati;
- all'acquisto e alla vendita di oro e/o metalli preziosi, oltre all'importo totale del valore degli acquisti e delle vendite, il numero totale delle operazioni effettuate.

[46] Le informazioni comunicate secondo il Decreto "Salva Italia", inclusive del valore medio di giacenza annuo di depositi e conti correnti bancari e postali, sono utilizzabili anche per la semplificazione degli adempimenti dei cittadini in merito alla compilazione della dichiarazione sostitutiva unica, concernente le notizie necessarie per la determinazione dell'indicatore della situazione economica equivalente (ISEE) ai fini della fruizione delle prestazioni sociali agevolate, nonché in sede di controllo sulla veridicità dei dati indicati nella medesima dichiarazione. Sul punto, si veda la disciplina attualmente contenuta all'art. 10, ottavo comma, del D.P.C.M. 05.12.2013 n. 159, regolamento concernente la revisione delle modalità di determinazione e i campi di applicazione dell'ISEE.

[47] Si tratta delle comunicazioni eseguite ai sensi tanto dell'art. 7, sesto comma, del D.P.R. 605/1973 (comunicazione mensile) quanto dell'art. 11, secondo comma, del D.L. 201/2011 (comunicazione integrativa annuale).

[48] Con il provvedimento del Direttore dell'Agenzia delle Entrate n. 18269 del 10.02.2015, l'archivio dei rapporti finanziari si è arricchito delle informazioni riguardanti la giacenza media dei rapporti (ovvero l'importo medio delle somme a credito del cliente in un dato periodo di tempo, ragguagliato all'anno).

[49] Si veda anche il successivo provvedimento dell'Agenzia delle Entrate n. 669173 datato 08.08.2019.

[50] Gli elenchi così formati, saranno diramati dalla Divisione Contribuenti alle competenti Direzioni regionali e provinciali, tramite un apposito applicativo informatico. Per ogni posizione segnalata, la Divisione comunicherà la numerosità dei conti correnti ed il totale aggregato dei saldi e dei movimenti dei rapporti nonché gli ulteriori elementi significativi presenti in Anagrafe tributaria. Le articolazioni territoriali destinatarie degli elenchi di propria competenza dovranno valutare ogni singola posizione segnalata, ai fini delle consuete attività di programmazione dei controlli, dandone specifico riscontro (*feedback*) alla medesima Divisione Contribuenti.

[51] Convertito in legge, con modificazioni, dall'art. 1, comma 1, della legge 17.12.2018, n. 136.

[52] Per Toschi (2018), p. 663, l'obiettivo di una forza di polizia economico-finanziaria a forte vocazione sociale, qual è la Guardia di finanza, resta prevenire, ricercare e reprimere i fenomeni illeciti con cui la delinquenza organizzata può inquinare o condizionare il corretto esercizio delle libertà economiche […] un moderno ed efficace contrasto a fenomeni così complessi richieda un approccio altrettanto trasversale e strutturato e, per questo, le linee d'azione del corpo si muovono lungo direttrici, fra loro integrate e complementari, quali [tra l'altro] l'esercizio

sull'art. 11 del D.L. 201/2011, "al fine di rafforzare le misure volte al contrasto dell'evasione fiscale" l'art. 16-*quater* (Disposizioni in materia di accesso all'archivio dei rapporti finanziari) ha disposto che:

- il provvedimento indicato al terzo comma, con il quale il Direttore dell'Agenzia delle entrate stabilisce le modalità di comunicazione periodica all'anagrafe tributaria, preveda "adeguate misure di sicurezza, di natura tecnica e organizzativa, per la trasmissione dei dati e per la relativa conservazione, che non può superare i dieci anni";
- le informazioni contenute nell'archivio dei rapporti finanziari oltre che ai fini previsti dall'art 7, undicesimo comma, del D.P.R. 605/1973 siano utilizzate per le analisi del rischio di evasione, oltre che dall'Agenzia delle entrate, come già previsto dal quarto comma, anche dalla Guardia di Finanza[53].

Nel contrasto all'evasione fiscale parimenti significative sono le disposizioni in materia di scambio automatico di informazioni contenute al successivo art. 16-*sexies*, primo comma, a norma del quale "l'Agenzia delle entrate fornisce, su richiesta, alla Guardia di finanza, per l'esecuzione delle attività di controllo tributario o per finalità di analisi del rischio di evasione fiscale, elementi e specifiche elaborazioni basate sulle informazioni ricevute ai sensi dell'art. 1, commi 145 e 146, della legge 28.12.2015, n. 208[54], nonché su quelle ricevute nell'ambito dello scambio automatico di informazioni per finalità fiscali previsto dalla direttiva 2011/16/UE del Consiglio, del 15.02.2011, e da accordi tra l'Italia e gli Stati esteri". Le disposizioni di quest'ultima direttiva, attuata con il d.lgs. 04.03.2014, n. 29, assumono particolare rilievo perché consentono all'Amministrazione finanziaria di disporre di un patrimonio informativo ulteriore, proveniente dalle omologhe Amministrazioni degli Stati membri dell'Unione europea, attraverso un differenziato sistema di scambio di informazioni[55].

L'ultimo profilo che esprime l'importanza dell'interoperabilità delle banche dati[56] e l'efficacia del sistema di prevenzione e contrasto dell'evasione fiscale e del riciclaggio dei proventi illeciti riguarda l'interazione tra la disciplina antiriciclaggio e le indagini fiscali[57].

A questo proposito, si è già fatto cenno alla possibilità di consultare l'archivio dei rapporti finanziari ai fini dell'approfondimento delle segnalazioni di operazioni sospette ai sensi del sesto comma degli artt. 6 e 9 del d.lgs. 231/2007. Queste disposizioni devono inoltre coordinarsi con l'art. 11, quarto comma, del D.L. 201/2011 a norma del quale le informazioni fornite dagli

combinato dei poteri di polizia economico-finanziaria, valutaria e giudiziaria; l'uso di tecnologie moderne per analisi "selettive" e "mirate"; la centralità dell'analisi dei flussi finanziari, aspetto fondamentale per legare le persone ai beni e viceversa".

[53] In questo caso, la relazione che l'Agenzia delle entrate trasmette annualmente alle Camere con i risultati relativi all'emersione dell'evasione a seguito dell'applicazione delle disposizioni relative all'archivio dei rapporti finanziari, deve contenere anche i risultati relativi all'attività svolta dalla Guardia di finanza utilizzando le medesime informazioni.

[54] La legge di stabilità 2016 ha introdotto a carico delle società controllanti (residenti in Italia) di gruppi multinazionali l'obbligo di predisporre e presentare annualmente una rendicontazione paese per paese (c.d. *Country-by-Country reporting*) recante l'ammontare dei ricavi e gli utili lordi, le imposte pagate e maturate, insieme con altri elementi indicatori di un'attività economica effettiva. In attuazione di tale previsione è stato adottato il D.M. 23.02.2017.

[55] Ai sensi del d.lgs. 29/2014, lo scambio può avvenire in base ad una specifica richiesta (art. 4), automaticamente per una serie di informazioni da comunicare obbligatoriamente (art. 5) oppure spontaneamente (art. 6). Sul tema si rinvia a Pitrone (2012), p. 463. L'orizzonte delle informazioni scambiabili nell'ambito della cooperazione amministrativa è stato recentemente ampliato con il d.lgs. 18.05.2018, n. 60, di attuazione della direttiva 2016/2258/UE del 06.12.2016, per quanto riguarda l'accesso da parte delle autorità fiscali alle informazioni in materia di antiriciclaggio. Nell'intervenire sull'art. 3 del d.l. 29/2014, il d.lgs. 60/2018 ha infatti previsto che:

- "i servizi di collegamento […] forniscono all'autorità richiedente dell'altro Stato membro tutti gli elementi utili per lo scambio di informazioni e la cooperazione amministrativa. A tal fine utilizzano i dati e le notizie acquisiti ai sensi del D.P.R. 29.09.1973, n. 605, e hanno accesso ai dati e alle informazioni sulla titolarità effettiva di persone giuridiche e trust, contenuti in apposita sezione del Registro delle imprese, di cui all'art. 21 del d.lgs. 21.11.2007, n. 231, con le modalità di cui al comma 2, lettera d), e al comma 4, lettera c), del medesimo articolo. […]" (terzo comma);
- ai fini delle "indagini amministrative di cui al comma 3, nell'ambito dell'esercizio dei poteri previsti dal Titolo IV del D.P.R. 29.09.1973, n. 600, agli uffici dell'Agenzia delle entrate e del Corpo della Guardia di finanza è consentito l'accesso ai documenti, ai dati e alle informazioni acquisiti in assolvimento dell'obbligo di adeguata verifica della clientela ai sensi dell'art. 18 del d.lgs. 21.11.2007, n. 231, con le modalità di cui all'art. 19 del predetto decreto legislativo, e conservati ai sensi dell'art. 31 con le modalità di cui all'art. 32 del medesimo decreto legislativo" (comma 3-*bis*).

Sul tema si rinvia a Carbone (2018), p. 3313.

[56] Tra gli strumenti a disposizione della Guardia di Finanza rientra anche il Sistema Informativo Antifrode (SIAF), una piattaforma informatica, sviluppata direttamente dal Corpo per migliorare l'analisi di rischio e così potenziare il contrasto alle frodi in danno del bilancio dell'Unione europea. In particolare, tale software integra i dati acquisiti da vari archivi informatici e fornisce elaborazioni con specifiche funzioni di "analisi" e "informative" per individuare posizioni soggettive o specifiche progettualità connotate da indici di anomalia sulle quali effettuare, prima dell'avvio degli eventuali controlli, opportuni riscontri. Senato della Repubblica (2017), p. 88.

[57] Per l'approfondimento si veda Borrelli (2016), p. 707.

operatori all'archivio dei rapporti finanziari ai sensi tanto dell'art. 7, sesto comma, del D.P.R. 605/1973 (comunicazione mensile) quanto dell'art. 11, secondo comma, del D.L. 201/2011 (comunicazione integrativa annuale) sono utilizzate anche per le finalità previste dall'art. 7, undicesimo comma, del D.P.R. 605/1973.

Con una formulazione che non brilla per coordinamento sistematico, ciò significa che nell'esercizio delle rispettive funzioni antiriciclaggio l'Unità di informazione finanziaria, la DIA ed il Nucleo speciale di polizia valutaria della Guardia di finanza vedono notevolmente accresciuto il patrimonio conoscitivo dei dati finanziari[58]. Tale interscambio è tuttavia bidirezionale nella misura in cui la disciplina antiriciclaggio prevede due disposizioni che rendono utilizzabili ai fini fiscali tutte le informazioni acquisite dalla Guardia di Finanza nell'ambito delle ispezioni e controlli e dell'approfondimento delle segnalazioni di operazioni sospette (art. 9, nono comma) nonché quelle conservate[59] dai soggetti obbligati (art. 34, primo comma).

5. L'acquisizione della notizia di reato "a tavolino".

La consultazione dell'archivio dei rapporti finanziari e, più generalmente, delle banche dati disponibili per l'Amministrazione finanziaria potrebbe far emergere indizi di reato per il superamento di soglie di rilevanza penale[60], anche al di fuori della materia tributaria[61].

Tale evenienza è particolarmente significativa per gli appartenenti al Corpo della Guardia di Finanza, che cumulano le funzioni di polizia economico-finanziaria e di polizia giudiziaria, e pone la necessità dell'osservanza dell'art. 220 disp. att. c.p.p. a norma del quale "quando nel corso di attività ispettive o di vigilanza previste da leggi o decreti emergono indizi di reato, gli atti necessari per assicurare le fonti di prova e raccogliere quant'altro possa servire per l'applicazione della legge penale sono compiuti con l'osservanza delle disposizioni del codice".

Se per le Sezioni Unite, infatti, il presupposto di operatività dell'art. 220 disp. att. deve rinvenirsi nella "mera possibilità di attribuire comunque rilevanza penale al fatto che emerge dall'inchiesta amministrativa e nel momento in cui emerge, a prescindere dalla circostanza che esso possa essere riferito ad una persona determinata"[62], occorre rilevare che, per almeno due ordini di motivi, l'accennata evenienza non presenta di criticità in ordine alle regole di comportamento che gli operatori devono osservare all'emergere degli indizi di reato né alla connessa garanzia di inutilizzabilità, come ricavabili dal citato art. 220[63]: da una parte, infatti, le informazioni acquisite all'anagrafe tributaria rilevano ai sensi e per gli effetti dell'art. 234 c.p.p.[64]; dall'altra, perché il profilo di maggiore interesse riguarda la possibilità di acquisire la notizia di reato anche "a tavolino"[65], attraverso il mero incrocio degli elementi disponibili alle banche dati[66].

[58] In questi termini Carbone (2013), p. 2356.

[59] Ai sensi dell'art. 31 (Obblighi di conservazione) del d.lgs. 231/2007 "2. […]. La documentazione conservata deve consentire, quanto meno, di ricostruire univocamente: a) la data di instaurazione del rapporto continuativo o del conferimento dell'incarico; b) i dati identificativi del cliente, del titolare effettivo e dell'esecutore e le informazioni sullo scopo e la natura del rapporto o della prestazione; c) la data, l'importo e la causale dell'operazione; d) i mezzi di pagamento utilizzati. 3. I documenti, i dati e le informazioni acquisiti sono conservati per un periodo di 10 anni dalla cessazione del rapporto continuativo, della prestazione professionale o dall'esecuzione dell'operazione occasionale".

[60] Secondo la Suprema Corte, durante una verifica fiscale, gli indizi del reato di dichiarazione infedele devono considerarsi emersi non all'avvenuto superamento della soglia di imposta evasa, bensì ancor prima, alla concreta probabilità che la medesima sia superata. Così Cass. pen., Sez. III, sent. n. 4919/2015. Rafaraci (2015), p. 675.

[61] Non soltanto le soglie rilevanti ai sensi degli artt. 4 (Dichiarazione infedele) e 5 (Omessa dichiarazione) del d.lgs. 74/2000, ma anche quella dell'art. 316-*ter* (Indebita percezione di erogazioni a danno dello Stato), tenuto conto che l'archivio dei rapporti finanziari consente di controllare la veridicità della dichiarazione sostitutiva unica, concernente le notizie necessarie per la determinazione dell'ISEE ai fini della fruizione delle prestazioni sociali agevolate.

[62] Così Cass. pen., Sez. Unite, n. 45477/2001. Izzo (2002), p.1178.

[63] Sul tema si veda Sorbello (2016b), p. 125.

[64] Art. 234 (Prova documentale) c.p.p.: "1. È consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo. […]".

[65] La verifica del superamento delle soglie di punibilità penali per le violazioni fiscali può avvenire anche "a tavolino". La Suprema Corte ha infatti ritenuto legittima la condanna inflitta dopo che la Guardia di Finanza ha determinato l'imposta evasa da una società incrociando le fatture attive e passive presenti nelle banche dati dell'amministrazione finanziaria. Se il contribuente non produce alcuna documentazione volta a "smontare" i conteggi dei verificatori, la determinazione dell'imposta evasa è infatti sufficiente a sorreggere il verdetto di colpevolezza. Così Cass. pen., Sez. III, sent. n. 7871/2019.

[66] Un chiaro esempio riguarda l'omesso versamento dell'IVA di cui all'art. 10-*ter* del d.lgs. 74/2000, "entro il termine per il versamento dell'acconto relativo al periodo d'imposta successivo, l'imposta sul valore aggiunto dovuta in base alla dichiarazione annuale" allorquando l'importo superi la soglia di € 250.000 per ciascun periodo d'imposta. Nel caso di specie, seppur dichiara il proprio debito IVA, il contribuente non effettua il relativo versamento entro il 27 dicembre dell'anno successivo, come previsto all'art. 6, secondo comma, della legge 29.12.1990,

Diversamente dall'approccio investigativo tradizionale, basato su conoscenza del territorio, osservazione e deduzioni, le nuove tecnologie mettono a disposizione dell'investigatore un ampio patrimonio informativo disponibile per orientare l'attività operativa in maniera selettiva e proficua.

La progressiva espansione dell'utilizzo dell'archivio dei rapporti finanziari e la corrispondenza biunivoca con la disciplina antiriciclaggio rappresentano una significativa leva di politica criminale perché arricchiscono gli strumenti di prevenzione e repressione della criminalità del reato, anche se ne risulta compressa la sfera privata dei contribuenti: la consultazione dell'archivio può ormai avvenire anche in una fase di selezione precedente al controllo e non soltanto dopo che siano già emersi riscontri positivi di evasione da corroborare con le indagini finanziarie[67].

Una simile preoccupazione deve però essere ridimensionata da regole e principi che richiedono un necessario bilanciamento.

In primo luogo, ai sensi dell'art. 1 della Direttiva (UE) 2016/680[68], il diritto alla protezione dei dai personali riguarda la protezione delle persone fisiche con riguardo al trattamento eseguito da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati: la circostanza che la procedura sperimentale per l'analisi del rischio di evasione, prevista dai provvedimenti del Direttore dell'Agenzia delle Entrate, riguardi soltanto la posizione fiscale di società di persone e di capitali esclude che tali strumenti siano utilizzati nei riguardi delle persone fisiche.

In secondo luogo, anche con riferimento a queste ultime, la normativa dell'Unione europea ci ricorda che "il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità"[69]. Tale esigenza di bilanciamento, come rilevabile nel preambolo della Direttiva (UE) 2016/680, riguarda anche le attività di polizia che "vertono principalmente sulla prevenzione, l'indagine, l'accertamento o il perseguimento di reati, comprese [quelle] condotte senza previa conoscenza della rilevanza penale di un fatto [e] per la salvaguardia contro e la prevenzione di minacce […] agli interessi fondamentali della società tutelati dalla legge che possono dar luogo a reati (12)", ivi incluso anche l'interesse erariale rilevante ai sensi degli artt. 2 e 53 della Costituzione. Nel perseguire tali finalità occorre "che le autorità competenti trattino i dati personali raccolti a fini di prevenzione, indagine, accertamento o perseguimento di specifici reati al di là di tale contesto per sviluppare conoscenze delle attività criminali e mettere in collegamento i diversi reati accertati (27)": si tratta dell'analisi di rischio effettuata anche grazie al trattamento automatizzato dei dati personali[70].

È di tutta evidenza che una simile compressione del diritto alla protezione dei dati personali è da ritenersi lecita fintanto che il trattamento avvenga "per finalità determinate, esplicite e legittime [non] incompatibili con le finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica (29)": soltanto in questo caso, infatti, il trattamento avviene "per l'esecuzione di un compito svolto nell'interesse pubblico (35)", in assenza del quale la consultazione delle banche dati avrebbe rilevanza penale[71].

Le nuove tecnologie consentono di analizzare e confrontare dati, restituendo una sintesi di informazioni complesse per orientare le attività di contrasto: alla tradizionale ricerca della notizia di reato, si affianca ormai anche l'analisi dei metadati, cioè del sistema delle relazioni fra dati singolarmente non significativi. L'automatico incrocio delle informazioni contenu-

n. 405: per l'accertare il reato, alla scadenza del termine, sarà sufficiente individuare i debiti IVA d'importo superiore alla soglia di rilevanza penale e riscontrarne l'omesso versamento mediante l'esclusiva consultazione dell'anagrafe tributaria.

[67] Così Carbone (2013), p. 2356.

[68] Al quale corrisponde l'art. 1 del d.lgs. 51/2018 di attuazione.

[69] Considerando n. 04 del Regolamento UE 679/2016.

[70] Il trattamento riguarda "qualsiasi operazione o insieme di operazioni compiute nei confronti di dati personali o insiemi di dati personali, con l'ausilio di strumenti automatizzati o in altro modo, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, il raffronto o l'interconnessione, la limitazione del trattamento, la cancellazione o la distruzione" (34).

[71] Secondo le Sezioni Unite, infatti, "integra il delitto previsto dall'art. 615-*ter* c.p., comma 2, n. 1, la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita". Cass. pen., Sez. Unite, sent. 41210/2017. Flor (2018), p. 506.

te nell'archivio dei rapporti finanziari con gli ammontari dichiarati ai fini delle imposte sui redditi permette in alcuni casi di acquisire pressoché immediatamente la notizia di reato (ad esempio quello tributario), senza che l'illecito si scopra quando è ormai prossima la prescrizione.

Bibliografia:

Acconci, Angela (1994): *Ordinamento penitenziario e criminalità organizzata al vaglio della Corte costituzionale* (nota a Corte cost., sent. 08.07.1993, n. 306), *Cass. pen.*, 4, pp. 861-870

Angiolini, Vittorio (1992): *Riserva di giurisdizione e libertà costituzionali* (Padova, Cedam)

Aprati, Roberta (2010): *La notizia di reato nella dinamica del procedimento penale* (Napoli, Jovene)

Beccaria, Cesare (1984): *Dei delitti e delle pene*, in Firpo, Luigi (direttore), *Edizione nazionale delle opere di Cesare Beccaria* (Milano, Mediobanca).

Becker, Gary: (1968): Crime and Punishment: An Economic Approach, in Journal of Political Economy, 2, pp. 169-217

Borrelli, Paolo (2016): *I riflessi della normativa antiriciclaggio sulle indagini finanziarie ai fini fiscali*, *Il Fisco*, 8, pp. 707-712

Calabresi, Guido (1961): Some thoughts on risk distribution and the law of torts, in The Yale Law Journal, 4, pp. 499-553

Carbone, Michele (2013): *Archivio dei rapporti finanziari: esigenze di razionalizzazione tra normativa fiscale e antiriciclaggio*, *Corr. trib.*, 30, pp. 2356-2372

Carbone, Michele (2018): *Accesso dell'Amministrazione finanziaria alle informazioni antiriciclaggio*, *Il Fisco*, 35, pp. 3313-3340

Centonze, Francesco (2011): *La "*partnership*" pubblico-privato nella prevenzione del riciclaggio e il problema della posizione di garanzia dei componenti degli organi di controllo societari*, in Aa.Vv., *Studi in onore di Mario Romano* (Napoli, Jovene) pp. 1757-1800

Cerri, Augusto (1990): *Ordine pubblico* (Diritto costituzionale), *Enc. giur.*, XII (Roma, Treccani).

Coase, Ronald (1960): The problem of social cost, in The Journal of Law and Economics, 3, pp. 1-44

Comando Generale della Guardia di Finanza (2018): *Manuale operativo in materia di contrasto all'evasione e alle frodi fiscali* (Roma)

Corso, Guido (1990): *Fine della polizia amministrativa?* (nota a Corte cost., sent. 04.04.1990, n. 162), *Giur. cost.*, 4, pp. 1006-1009

Corso, Guido (1996): *Polizia di sicurezza*, in *Dig. disc. pubb.*, XI, pp. 319-336

Donini, Massimo e Pavarini, Massimo (2011), *Sicurezza e diritto penale* (Bologna, Bononia University Press)

Falsitta, Gaspare (1992): *Epicedio per il segreto bancario nei confronti del Fisco* (nota a Corte cost., sent. 03.02.1992, n. 51), in *Riv. dir. trib.*, 2, pp. 566-569

Falsitta, Gaspare (2003): *I condoni fiscali tra rottura di regole costituzionali e violazioni comunitarie*, in *Il fisco*, 6, pp. 794-804

Fiandaca, Giovanni (1990): *Pena "patteggiata" e principio rieducativo: un arduo compromesso tra logica di parte e controllo giudiziale* (nota a Corte cost., sent. 02.07.1990, n. 313), in *Foro it.*, I, pp. 2385-2393

Flick, Giovanni Maria (2015): Governance *e prevenzione della corruzione: dal pubblico al privato o viceversa?*, in *Riv. AIC*, 2

Flor, Roberto (2018): *La condotta del pubblico ufficiale fra violazione della* voluntas domini, *"abuso" dei profili autorizzativi e "sviamento di potere"* (nota a Cass. pen., Sez. Unite, sent. 08.09.2017, n. 41210), in *Dir. pen. proc.*, 4, pp. 506-515

Giupponi T., *Sicurezza personale, sicurezza collettiva e misure di prevenzione. La tutela dei diritti fondamentali e l'attività di intelligence*. Intervento al Seminario "Sicurezza collettiva e diritti fondamentali" dell'Università di Ferrara, 26.09.2007, in www.forumcostituzionale.it.

Hobbes, Thomas (2011): *Leviatano* (trad. Micheli G., Milano, Bur Rizzoli)

Izzo, Gioacchino (2002): *Le sezioni Unite limitano l'utilizzabilità di dichiarazioni rese in sede ispettiva di vigilanza*, in *Il fisco*, pp. 1178-1180

Leone, Stefania (2006): *La "zona rossa" dei diritti: considerazioni sulla legittimità delle ordinanze del Prefetto "di necessità ed urgenza", a margine di una recente sentenza del Consiglio di Stato* (nota a Cons. Stato, Sez. VI, sent. 16.01.2006, n. 85), in *Giur. cost.*, 5, pp. 3479-3511

Locke, John, *Due trattati sul governo* (trad. Casalini B., Pisa, Ed. Plus, 2007)

Mantovani, Ferrando (2006): *La "perenne crisi" e "la perenne vitalità" della pena. E la "crisi di solitudine" del diritto penale,* in Dolcini Emilio e Paliero Carlo Enrico (a cura di), *Studi in onore di Giorgio Marinucci,* I (Milano, Giuffré), pp. 1171-1212

Martini, Adriano (2010): *Reati in materia di finanze e tributi*, in Grosso Carlo Federico, Padovani Tullio, Pagliaro Antonio (diretto da), *Trattato di diritto penale* (Milano, Giuffré).

Ministro dell'economia e delle finanze (2007), *I risultati della lotta all'evasione. Relazione al Parlamento* (Roma)

Montesquieu C.L., *Lo spirito delle leggi* (trad. Boffitto Serra B., Milano, 1967).

Musco, Enzo (2007): *Reati tributari* (voce), in *Enc. del diritto*, Annali (Milano, Giuffré), 1039-1065

Nova, Antonio (1996): *Polizia amministrativa*, in *Dig. disc. pubb.*, XI (Torino, Utet)

Nuvolone, Pietro (1956): *Appunti e spunti tra precetti e sanzioni* (nota a Corte cost., sent. 23.02.1956, n. 2), in *Riv. it. dir. pen.*, p. 441

Paliero, Carlo Enrico (2005): *L'economia della pena (un* work in progress*),* in *Riv. it. dir. proc. pen.*, 4, pp. 1336-1401

Pitrone, Federica (2012): *Lo scambio di informazioni e la direttiva 2011/16UE in materia di cooperazione amministrativa: innovazioni e profili critici*, in *Dir. e prat. trib. intern.*, 2, pp. 463-491

Pulitanò, Domenico (2009): *Sicurezza e diritto penale*, in *Riv. it. dir. proc. pen.*, 2, pp. 547-568

Rafaraci, Tommaso (2015): *Reati tributari con soglia di punibilità e applicazione dell'art. 220 disp. att. c.p.p.: la Cassazione rimarca i diritti della difesa* (nota a Cass. pen., Sez. III, sent. 03.02.2015, n. 4919), in *Riv. Guardia di Finanza*, 3, pp. 673-687

Ricozzi, Carlo e Di Paolo, Nino (2003): *La funzione di polizia economica e finanziaria*, in *Riv. Guardia di Finanza*, 5, pp. 1485-1504

Risicato, Lucia (2019): *Diritto alla sicurezza e sicurezza dei diritti: un ossimoro invincibile?*, (Torino, Giappichelli)

Senato della Repubblica (2017): *Lotta alle frodi in danno delle uscite di bilancio dell'Unione europea*, pp. 1-117.

Sorbello, Pietro (2016a): *La valutazione di sospetti, indizi e notizie di reato nel passaggio (incerto) dalle attività ispettive alle funzioni di polizia giudiziaria*, in *Riv. trim. dir. pen. cont.*, 2, pp. 125-135

Sorbello, Pietro (2016b): *Politica criminale ed osservanza delle regole. Riflessioni su limiti e possibilità di conversione al razionale dei comportamenti*, in *Riv. it. dir. proc. pen.*, 4, pp. 1914-1948

Sorbello, Pietro (2015), *Segnalazione di operazioni sospette e posizione di garanzia. Ammissibilità e limiti del concorso per omissione nel delitto di riciclaggio*, in *Ind. pen.*, 3, pp. 437-471

Soro, Antonello (2017): *Proteggere i dati per governare la complessità*. Discorso del Presidente dell'Autorità garante per la protezione dei dati personali. Relazione (Roma)

Tesauro, Francesco (2011): *Istituzioni di diritto tributario* (Torino, Utet)

Toschi, Giorgio (2018): *Il metodo Falcone: dalla prime indagini bancarie alle attuali investigazioni economico-finanziarie*, in *Riv. Guardia di Finanza*, 3, pp. 663-668

Travi, Aldo (1988): *Definizione legale delle materie e principio di ragionevolezza: il caso della polizia mineraria*, in *Le regioni*, 3, pp. 830-840

Tridico, Bruno Domenico (2017): *L'utilizzo dell'anagrafe dei rapporti finanziari ai fini dell'attività di controllo fiscale*, Relazione Corte dei Conti – Sez. centrale di controllo sulla gestione delle Amministrazioni dello Stato (Del. 26.07.2017, n. 11/2017/G)

Vassalli, Giuliano (2007): *Introduzione a "diritto penale giurisprudenza costituzionale"*, in Id., *Ultimi scritti* (Milano, Giuffé)

Nuove tecnologie e processo penale

Nuevas tecnologías y proceso penal

New Technologies and Criminal Procedure

Algoritmi predittivi: alcune premesse metodologiche

Algoritmos predictivos: algunas premisas metodológicas

Predictive Algorithms: Some Methodological Considerations

Barbara Occhiuzzi
Dottoranda di ricerca, Scuola Universitaria Superiore Sant'Anna di Pisa
barbara.occhiuzzi@santannapisa.it

Intelligenza artificiale | Inteligencia artificial | Artificial Intelligence

Abstracts

Il ricorso all'automatizzazione nei processi decisionali offre numerosi vantaggi ma la complessità del procedimento renderebbe gli esiti difficilmente prevedibili. Occorre, dunque, domandarsi se l'avvento delle nuove tecnologie imponga un ripensamento delle categorie fondamentali del diritto e del processo penale.

El recurso a la automatización en los procesos de toma de decisión plantea numerosas ventajas. Sin embargo, la complejidad del procedimiento presenta el riesgo de convertir sus resultados en altamente imprevisibles. Es necesario, por tanto, preguntarse si el advenimiento de las nuevas tecnologías impone un repensamiento de las categorías fundamentales del derecho y del proceso penal.

The use of automation in the decision-making processes has several values but the complexity of the machine – learning procedure would make the results difficult to predict. It is therefore necessary to ask whether the advent of new technologies requires a rethinking of the fundamental categories of law and the criminal trial.

Sommario

1. Algoritmi e processo decisionale: i termini di un *rinnovato* dibattito metodologico.

«Ecco un esercizio per voi: la prossima volta che sentirete qualcuno parlare di algoritmi, sostituite questo termine con 'Dio' e domandatevi se il significato cambia[1]».

La percezione di un ricorso pervasivo a meccanismi decisionali automatizzati, nelle parole degli studiosi, dei tecnici e dell'opinione pubblica, rivela oggi alcuni caratteri peculiari di un fenomeno tanto esteso quanto, paradossalmente, ancora in gran parte inesplorato. La sensazione dominante è che quanto più l'impiego di simili strumenti di elaborazione dati si diffonda, tanto più di tale utilizzo si apprezzi la naturale necessità, pure avallata dai vantaggi dell'efficienza, e tuttavia accompagnata, in modo direttamente proporzionale, dalla percezione dell'ignoto, di una imperscrutabilità propria di ciò che, per definizione, è ovunque ed in ogni luogo, al punto da sovrintendere processi elementari quanto complessi. In questo senso, l'accostamento dell'algoritmo alla *divinità* si rivela un'immagine particolarmente efficace: gli algoritmi sono ovunque ed operano in modo imperscrutabile.

Fuor di metafora, il successo di questo particolare procedimento automatizzato di elaborazione di informazioni si fonda, in particolare, sul grado di rendimento che, grazie alla rapidità, in primo luogo, si dimostra particolarmente elevato, in larga misura più efficiente di un qualsiasi metodo alternativo di analisi di informazioni, primo tra tutti, l'attività naturale di elaborazione, valutazione e selezione che è in grado di compiere l'uomo.

Se dunque il livello di diffusione degli algoritmi nella vita di tutti i giorni è debitore del grado di utilità che esso garantisce, la componente di "ignoto" connaturale all'impiego dei più sofisticati metodi computazionali, è parimenti un frutto del progresso tecnologico. Si tratta di un progresso che supera se stesso e si contraddice, si fonda sulla conoscenza fino a negarla, culmina nella c.d. *black box*, limite alla comprensione della scelte operate dalla macchina. Gli algoritmi predittivi si collocano in una particolare area dell'informatica che utilizza la ricerca automatizzata di correlazioni e collegamenti per giungere ad una decisione e fondare delle scelte. Tale capacità, del tutto simile, in via elementare, al meccanismo della più semplice facoltà di scegliere propria dell'individuo, ha conosciuto, negli ultimi anni, un repentino *replacement* da parte delle macchine rispetto alle competenze umane[2], da ultimo, in campo giuridico, riservando conseguenze del tutto inattese e con le quali occorre oggi confrontarsi[3]. Tale difficoltà deriva da un'evidenza drammatica: nei procedimenti particolarmente complessi di analisi dei dati, le correlazioni ed i collegamenti funzionali a pervenire al risultato ed alla scelta selezionata non sono riconoscibili, ed il percorso motivazionale, la struttura e finanche il contenuto, resta, di fatto, ignoto.

Lungi dal voler semplificare la complessità di un fenomeno ampio quanto eterogeneo, quale l'impiego di algoritmi predittivi in ambito giuridico, si intende qui compiere un tentativo di definizione e razionalizzazione delle problematiche future e attuali, che si pongono in primo luogo all'attenzione del giurista che intenda misurarsi sino ai confini delle più avanzate latitudini tecnologiche. Da una parte sarà opportuno chiarire la definizione quanto la funzione dei momenti che compongono i processi decisionali automatizzati, e specularmente domandarsi se quelle medesime componenti, per caratteristiche e scopo, siano funzionali ad assolvere una *qualsiasi* attività critica di scelta, selezione e decisione cui si pervenga in ambito giuridico. Un simile esercizio, a ben vedere, sarà funzionale non soltanto all'interprete per conoscere e comprendere un fenomeno nuovo ma anche e soprattutto ad avere contezza di istituzioni e principi di diritto fondamentali, quanto risalenti nel tempo, e di importanza sistematica all'interno del nostro ordinamento giuridico. Si devono intendere in quanto tali

[1] Bogost (2015), p. 1.
[2] Sheppard (2015), p. 1790.
[3] Casey e Niblett (2016), pp. 429-42; Alarie (2016), pp. 443–55.

precisamente i meccanismi in cui operano gli algoritmi predittivi: e-disclosure, ricerca e analisi forense, valutazione delle prove, ricerca, analisi e selezione della giurisprudenza rilevante, delle argomentazioni e della legge applicabile[4].

Il presente lavoro intende approfondire, in ipotesi, le potenzialità ed i limiti propri di uno modello particolarmente efficace di elaborazione dei dati e delle informazioni in ambito giuridico. Il diritto penale si rivela in tal senso una prospettiva di indagine privilegiata, non solo per l'esperienza concreta che negli Stati Uniti ha avuto ad oggi l'utilizzo degli algoritmi predittivi, ma anche e soprattutto per il carattere fondamentale ed insuperabile dei principi direttamente interessati dall'impiego di tali strumenti, attinenti, in ultima analisi, alla determinazione ed alla valutazione dell'area del penalmente rilevante.

La dottrina più attenta in materia ha già inteso, in tal senso, superare il dato empirico delle problematiche emerse dall'impiego di algoritmi predittivi, relative al rischio di violazione dei diritti umani e della privacy, per osservare il fenomeno dall'alto e coglierne le potenzialità operative in concreto, legate all'impiego dei sistemi computazionali avanzati nella formulazione, nell'interpretazione del precetto normativo e nell'argomentazione delle decisioni[5].

L'impiego di algoritmi predittivi e processi decisionali automatizzati nel procedimento penale, salvo costituire un'esperienza del tutto peculiare in materia di giudizio di pericolosità sociale (da doversi tuttavia doverosamente circoscrivere alla particolarissima esperienza statunitense), ai fini della presente trattazione rappresenta, prima di tutto, un modello.

Per inciso, un modello matematico, di natura statistico - probabilistica, che pretende di costituire un metodo garante di oggettività in precise componenti del procedimento penale. La possibilità che un preciso calcolo matematico pervenga a determinare il livello di pericolosità sociale di un individuo, riesca a ponderare il rischio di recidiva e sia ragionevolmente in grado di sostituirsi al giudice nel fondare una sentenza di condanna, prima che un ideale illuministico, sembra oggi essere divenuta una realtà storica.

Gli algoritmi predittivi sono utilizzati da anni negli Stati Uniti, e da qualche tempo anche in Europa[6], in specifici momenti del procedimento penale. Nulla ad oggi esclude che per loro natura, per i compiti e la funzione che adempiono, questi processori automatici di informazioni possano un giorno sostituirsi del tutto all'attività giudiziale, portando con sé vantaggi e dilemmi in grado di riscrivere o finanche superare principi fondanti il nostro sistema penale.

In primo luogo, l'esperienza ad oggi insegna che, per quanto 'futurisco' ed impensabile possa apparire l'impiego di una macchina al posto di un giudice, se non altro per l'incognita teorica dei possibili risvolti che questo possa comportare, per ciò solo non è dato di poter escludere che una simile circostanza si realizzi. In altre parole, lo stato dell'arte tradisce, accanto ad una diffusione dilagante di tali strumenti, un livello di teorizzazione ancora agli esordi[7], impegnato non solo a risolvere le problematiche metodologiche da essa derivanti, ma finanche i risvolti del tutto ignoti che (forse) soltanto l'esperienza, appunto, poteva presentare. In tale ambito può dirsi davvero che 'la realtà supera la fantasia', là dove l'immaginazione, intesa come grado di approfondimento teorico, deve ancora confrontarsi con una realtà ad uno stadio avanzato di operatività, carente di regolamentazione e, per ciò solo, di fatto, imprevedibile.

Ed ecco che ad un livello di teorizzazione approfondito emergono interrogativi elementari: « il vero problema non è la *black box*, che è molto più neutrale delle decisioni umane che sostituisce: dobbiamo programmare il nostro algoritmo in un mondo permeato dall'eredità della discriminazione passata e dalla realtà delle discriminazioni presenti» [8]. A ben vedere, le novità che la tecnologia applicata al diritto presenta, altro non sono, in larga misura per il dibattito teorico giuridico chiamato ad analizzarle, che l'epifania di questioni fondamentali ed "eterne", che proprio sui banchi del futuro tornano a manifestarsi. Non a caso, la dottrina internazionale già 'esperta' in materia ha riconosciuto questa familiarità con dilemmi antichi: «per coloro che sono avvezzi con il paradosso della *Rule of* Law, quella degli algoritmi è una sfida familiare»[9].

La prospettiva del diritto penale ha una ragion d'essere del tutto peculiare nel dibattito in questione, per due ordini di ragioni. Perché esiste un'esperienza concreta di algoritmi predit-

[4] Susskind (2010), p. 242; Katz (2013), p. 910.
[5] Hildebrandt (2018), pp. 12-35; Alarie (2016), pp. 443-455.
[6] Oswald *et al.* (2018), pp. 223-250; Urwin (2017), p. 4.
[7] Council of Europe (2017), p. 10-34.
[8] Pande (2018); Leight Brown (2015).
[9] Hildebrandt (2018), p.16.

tivi applicati al procedimento penale e, nello specifico, né è un chiaro esempio l'impiego dei medesimi nei meccanismi di *risk assessment* in molti tribunali degli Stati Uniti, dunque nei processi di valutazione del giudizio di pericolosità sociale. In secondo luogo, perché nel diritto penale, più che in ogni altra branca del diritto, proprio la pretesa di oggettività nei momenti tipicamente discrezionali ha una valenza insuperabile che, in quanto tale, necessita di essere definita e valorizzata negli strumenti che intendano garantirla.

L'algoritmo predittivo in ambito giuridico replica un'operazione tipicamente umana: apprendere informazioni, comunicare dei risultati, finalizzare la propria ricerca e prendere una decisione. La giustizia predittiva, nel senso più elementare del termine, consiste nell'anticipazione di una decisione, nella previsione di un risultato. L'algoritmo non fa altro che replicare attività naturalmente umane, in modo più rapido ed efficiente, analizzando e selezionando una vasta quantità di informazioni. Per questo motivo l'impiego di algoritmi predittivi è un riflesso della tecnologia applicata al diritto sostanziale di portata sistemica. L'algoritmo predittivo in ambito giuridico è suscettibile di declinarsi in una giustizia predittiva, che in quanto tale è "una giustizia anticipata". In definitiva, una giustizia *prevedibile*[10].

Non è tuttavia soltanto nel momento interpretativo che si può apprezzare, in astratto, il contributo agevolatore di un procedimento automatizzato di elaborazione dati. A ben vedere, l'impiego di algoritmi predittivi in ambito giuridico, proprio perché concepiti per replicare un meccanismo elementare, è potenzialmente sterminato. Eppure, non tutte le problematiche sono le medesime. Per questa ragione, occorre procedere per gradi ed operare una selezione degli ambiti in cui un meccanismo automatico possa ragionevolmente rivelarsi sufficiente a determinare una scelta, dalle ipotesi in cui il medesimo strumento sia funzionale a coadiuvare, semplicemente, le decisioni dell'uomo.

In questo si pone una questione centrale nel dibattito sugli algoritmi, da intendersi alla stregua di un problema di carattere definitorio. Per tale si deve intendere la valutazione e la selezione, la determinazione, appunto, dell'ambito di operatività degli algoritmi predittivi. Di fronte alla possibilità di un impiego concreto di meccanismi decisionali automatizzati nel procedimento penale, il giurista è chiamato a confrontarsi con un lessico tecnico e delle conoscenze nuove che richiedono una nuova *formazione*. L'esperienza concreta nelle corti degli Stati Uniti ha disvelato un problema, non trascurabile e non isolato. Ma la pluralità di problemi si intuisce nell'ampio spettro di situazioni in cui un processo decisionale automatizzato potrebbe coadiuvare i normali metodi di elaborazione e valutazione di informazioni utilizzati dall'uomo.

2. L'esperienza d'oltreoceano sugli algoritmi predittivi impiegati nell'ambito del *risk assessment*.

Negli Stati Uniti gli algoritmi predittivi hanno fatto la propria comparsa, in termini problematici, più di una decina di anni fa. Il dibattito teorico si è acceso con il caso *State v. Loomis*[11], nel 2016. In tale circostanza, la Corte Suprema del Wisconsin ha stabilito che l'impiego di algoritmi predittivi per la valutazione del rischio di recidiva non viola il diritto dell'imputato ad un equo processo.

Dall'esperienza *Loomis* ha preso le mosse il dibattito relativo non solo alle implicazioni etico-legali dell'impiego di algoritmi predittivi nei percorsi decisionali giudiziali, ma anche in merito alla possibilità del medesimo sistema di coinvolgere momenti ulteriori del procedimento penale, ugualmente attinenti alla fase successiva a quella di merito (*trial*) e relativa, per l'appunto, alla commisurazione della pena (*sentencing*).

È singolare osservare alcuni profili di somiglianza tra le problematiche interpretative tipiche di un determinato momento discretivo del processo penale e le principali questioni giuridiche in materia di algoritmi predittivi. In altre parole, a partire dal caso *Loomis* si è palesata, suscitando lo stupore generale, una peculiare fallacia dei processi decisionali automatizzati: la possibilità che questi arrivino a suggerire giudizi poco accurati, non motivati e finanche discriminatori[12].

Proprio il margine di straordinaria discrezionalità del giudice è un tratto storicamente

[10] Montedoro (2018).
[11] State v. Loomis, 881 N.W.2d 749 (Wisc. 2016).
[12] Angwin *et al.*, (2016).

caratteristico dei metodi di commisurazione della pena che si sono avvicendati nell'esperienza statunitense[13]. Si deve ritenere che l'utilizzo di algoritmi predittivi, in generale, sia uno dei frutti dell'ampio dibattito, protrattosi negli anni negli Stati Uniti, sul grado di obiettività del sistema di giustizia penale nel suo complesso[14]. L'impiego di strumenti di calcolo in tale ambito, affiancati dal ricorso a software e processi decisionali automatizzati, risulta oggi diffuso al momento dell'individuazione di programmi idonei di riabilitazione del detenuto, nella valutazione del rischio di recidiva, in fase cautelare e di determinazione della pena.

Proprio l'occasione del caso *Loomis* e, più in generale, l'ambito di applicazione dei software di valutazione della pericolosità sociale, sono funzionali a rivelare, insieme alle profonde differenze strutturali presenti tra l'ordinamento statunitense ed il nostro, l'incidenza, in concreto, di tali meccanismi all'interno di fasi del procedimento penale potenzialmente dotate di un significativo margine di discrezionalità da parte del giudice.

Nell'ordinamento italiano, l'imputazione formale è titolo e giustificazione sostanziale per l'impostazione della pena; la colpevolezza è *fondamento* e *limite* della pena e tale circostanza consente solo in parte di valutare la condotta concretamente rilevante ai fini della commisurazione e la personalità del reo[15]. Negli Stati Uniti la commisurazione della pena è affidata ad un secondo momento del procedimento penale, separato dalla fase di accertamento e di imputazione del fatto. È dunque e propriamente nella fase di commisurazione della pena, così come in quella di valutazione del livello di pericolosità sociale, che viene in considerazione la possibilità di impiegare gli algoritmi predittivi.

Tale circostanza impone una prima considerazione critica. Un meccanismo decisionale automatizzato, come quello garantito dall'impiego di algoritmi predittivi, è in grado di razionalizzare una quantità significativa di informazioni, dalle quali si ricava una soluzione che si fonda, essenzialmente, su un'analisi di tipo statistico – comparativo. Le tecniche più varie impiegate nell'ambito degli algoritmi predittivi e nei processi di *machine learning,* in generale, pongono in essere un 'trattamento informatico' (*computer processing*) del linguaggio umano (*Natural Language Processing)* in grado di sviluppare relazioni statisticamente accurate tra un *input* e un *output*. In altri termini, inserendo in un determinato *software* dei documenti determinati, siano questi attinenti a materiale probatorio od anche alla legislazione, alla dottrina od alla giurisprudenza, ad esempio, il *software* sarà in grado di fornire un documento pertinente alla ricerca richiesta, dunque di selezionare il materiale o i documenti pertinenti allo scopo[16].

In primo luogo, è precisamente la destinazione delle informazioni richieste, e dunque, ugualmente, di quelle fornite, a determinare un primo momento selettivo di fondamentale importanza. Una selezione che, a ben vedere, è necessariamente *esterna* al procedimento decisionale posto in essere dalla macchina. In altre parole, proprio la destinazione delle informazioni, della valutazione e dei risultati richiesti all'algoritmo è una prima variabile indipendente dall'algoritmo stesso, che il *software* non è in grado di determinare, è una componente necessariamente determinata dall'uomo.

L'attuale modello di commisurazione della pena, nel procedimento penale statunitense, nasce in misura significativa dalla necessità di porre un limite alla discrezionalità propria dell'*indeterminate sentencing* (una *multiple discretion,* non solo del giudice, ma anche del legislatore, del prosecutor e del *parole broad* [17]). In un primo momento, già a partire dalla fine del XIX secolo, le teorie votate alla rieducazione del condannato[18] avevano contribuito, di fatto, a focalizzare l'attenzione del giudice sull'individuazione di un trattamento sanzionatorio personalizzato, per questo fondato su un ampio spettro di informazioni sul destinatario[19] e, di fatto, orientato dall'incerta bussola dei «bisogni di risocializzazione del reo»[20]. Proprio a partire dalla stagione della rieducazione, si palesa, all'interno del sistema processuale americano, una forma eccezionale di discrezionalità in capo al giudice: la considerazione delle caratteristiche individuali, in luogo del mero riferimento al fatto commesso, aveva favorito una personalizzazione eccessiva nella commisurazione della pena, al punto da determinare decisioni discriminato-

[13] Stith e Cabranes, (1998), pp. 202 ss.
[14] Kehl *et al.* (2017), pp. 6 ss., Koepke e Robinson (2018), p. 1725.
[15] Dolcini (1979), p. 55; Conso (1968), pp. 706-712; Gianniti (1984), pp. 253 ss.
[16] Hildebrandt (2018), pp. 11.
[17] Zimring (1977), pp. 4ss.
[18] G. Mannozzi (1991), pp. 151 ss.; Hentig (1933-1934), p. 1081.
[19] O'Hear (2011), p.1292.
[20] Lopez (1981), p. 533; Radzinowicz e R. Hood (1979), p. 288.

rie[21].

Non da meno si dimostrano i risultati del *Sentencing Reform Act* del 1984, che prevede per le sentenze di commisurazione della pena una struttura determinata e delle linee guida vincolanti[22]. La fase del *sentencing* viene suddivisa, a questo punto, in due momenti ulteriori: uno dedicato alla raccolta di tutti gli elementi rilevanti, in generale, ai fini della commisurazione della pena, ed un secondo momento precisamente volto alla determinazione della pena nel singolo caso[23]. Mediante il ricorso alle linee guida[24], valutata la gravità del fatto a confronto con la capacità di delinquere del reo, il meccanismo del *determinate sentencing* è in grado di garantire una «pena giusta»[25], in relazione tanto al fatto commesso quanto alla personalità del condannato.

Il software COMPAS (*Correctional Offender Management Profiling for Alternative Sanction*) al centro del *leading case Loomis*, concepito per determinare il livello di pericolosità nella valutazione del rischio di recidiva, viene oggi utilizzato da alcuni Stati federali per coadiuvare il giudice nella commisurazione della pena. Tale circostanza è data dalla volontà di ricercare una maggiore equità della sanzione nella sua personalizzazione, da doversi valutare non solo alla luce delle caratteristiche proprie del condannato, ma anche in parametri esterni, che consentono di relativizzare la capacità a delinquere[26].

Nel caso *Loomis*, in particolare, il software COMPAS è stato utilizzato per determinare il rischio di recidiva del condannato (*recidivism risk assessments*), una voce propria di un documento di riepilogo sulla capacità a delinquere del condannato, funzionale a determinare la presenza di circostanze tali da attenuare o aggravare l'afflittività del trattamento sanzionatorio. Tali informazioni possono essere utilizzate per individuare un determinato programma di riabilitazione, l'istituto di destinazione del condannato, finanche determinare la durata della pena[27]. Non ultimo, i report di riepilogo della capacità a delinquere di un determinato condannato confluiscono nelle banche dati dei tribunali, e da *output* di un procedimento particolare divengono automaticamente *input* per un procedimento ulteriore.

Esiste una problematica tipica dei meccanismi decisionali automatizzati, che il caso *Loomis* ed, in particolare, l'inchiesta di ProPublica[28], hanno fatto emergere con drammatica chiarezza: la possibilità che il responso delle 'macchine pensanti' sia viziato da variabili discriminatorie. Tale circostanza è un rischio proprio del ricorso a strumenti algoritmici come COMPAS, in quanto, in primo luogo, la natura di brevetto propria dell'algoritmo brevettato che i meccanismi di funzionamento che ne governano le scelte siano resi pubblici[29]. Ne consegue che l'ipotesi che le soluzioni fornite dall'algoritmo siano "viziate" da elementi esterni alla valutazione richiesta non sia un dato facilmente verificabile.

L'evoluzione del caso COMPAS consente di rintracciare una prima risposta a questo genere di evenienza. La Corte Suprema del Wisconsin ha avvalorato l'impiego degli algoritmi predittivi in tema di *rsk assessment*, escludendo che questi potessero comportare una violazione del principio del giusto processo e finanche che i risultati cui questi erano pervenuti fossero discriminatori. Fatta salva la possibilità di giungere ad un perfezionamento dell'algoritmo tale da consentirne la verifica delle motivazioni, la Corte Suprema del Winsconsin ne ha legittimato l'impiego in astratto, non senza alcune riserve. Un assunto di principio deve dirsi di particolare rilevanza nel caso *Loomis:* il divieto che il giudice fondi la propria determinazione unicamente sulle risultanze dell'algoritmo, e che questi assisti l'attività decisoria, ma non arrivi sino ad escluderla.

[21] Kehl *et al* (2017), pp. 7 ss.
[22] Kehl *et al* (2017), pp. 7 ss.
[23] Mannozzi (1991), pp. 151 ss.
[24] James (2015), p. 13 ss.
[25] Mannozzi (1991), pp. 157 ss.
[26] Starr (2013), p. 800.
[27] Casey *et al* (2011), p. 33 ss.
[28] Angwin (2016).
[29] Eaglin (2017), pp. 67 ss; Starr (2013), p. 809.

3. *Actio finium regundorum* degli ambiti di applicazione e presupposti generali di operatività.

La legittimazione della sentenza *Loomis* in favore dell'utilizzo di algoritmi predittivi nel corso del procedimento penale non è priva di alcuni *caveat,* in larga misura di valenza generale rispetto alla possibilità che un meccanismo decisionale automatizzato assista il giudice nelle proprie scelte. Proprio l'attività di ausilio risulta, di fatto, l'unica opzione di impiego di fatto ammessa dalla Suprema Corte del Wisconsin nel *leading case*. La combinazione del contributo umano al processo valutativo e decisionale dell'algoritmo non si limita alla persona del giudice. Da una parte, la Corte Suprema del Winsconsin ha chiarito come il giudice possa legittimamente avvalersi del *software* per meglio comprendere la personalità del condannato e la sua capacità a delinquere, non già per determinare la pena e non senza che lo stesso giudice prenda parte alla medesima decisione[30]. Tale conclusione è comprensibile, da una parte, per via del fatto che l'algoritmo COMPAS non fosse stato concepito per analizzare tutte le componenti di giudizio nel *sentencing*[31], quanto per operare la sola valutazione del rischio di recidiva. D'altra parte, la natura statistico – comparativa del *software* impiegato non era in grado di garantire un giudizio del tutto personalizzato, ma solo la risultante dell'analisi di circostanze ed esperienze statisticamente simili. In altre parole, l'algoritmo non avrebbe potuto, da solo, determinare la sanzione e sostituirsi al giudice, in quanto «la valutazione del rischio recidiva da parte di COMPAS non esprime la probabilità specifica che un singolo autore possa nuovamente commettere il reato. Al contrario, fornisce una previsione basata sul confronto tra una serie di dati sul soggetto ed un insieme di informazioni simili»[32].

Tale premessa non ha impedito alla Corte di concludere che il giudizio riservato al signor *Loomis* fosse comunque fondato su informazioni veritiere, personalizzato e non discriminatorio. E tuttavia, in questo si scorge, nella sentenza, un ulteriore limite all'impiego di algoritmi predittivi, cui porre rimedio, nuovamente, mediante la "supervisione" di un soggetto persona fisica, questa volta l'imputato: la gran parte delle informazioni utilizzate dall'algoritmo derivavano da un questionario compilato dal medesimo e da registri pubblici, rispetto ai quali l'imputato aveva facoltà di assicurarsi che i dati in esso contenuti fossero corretti.

A ben vedere, non è, tuttavia, la correttezza o la veridicità dell'informazione a garantirne l'utilizzabilità ai fini della decisione e l'idoneità a fondare il giudizio, o almeno, non soltanto. In primo luogo, fintantoché la natura di brevetto registrato impedisce di ricostruire il percorso motivazionale fondativo della decisione, esiste un ostacolo insuperabile alla conoscibilità ed alla comprensione della medesima ed, in via generale, si deve ritenere, alla legittimità delle componenti del giudizio. Se anche questa si dovesse dimostrare una circostanza superabile, plausibilmente in ragione del diritto del condannato a conoscere il percorso motivazionale che fonda la sentenza, anche e soprattutto ai fini dell'impugnazione della decisione, l'idoneità degli elementi fondativi di una decisione non si misura soltanto sulla loro veridicità, sulla correttezza, appunto.

È la rilevanza attribuita a determinati elementi, direttamente connessi allo scopo delle valutazione, a fondare le ragioni di una determinata scelta. Esistono, in questo senso, componenti della decisione che non possono essere determinati dal procedimento decisionale in sé, ma costituiscono, di questo, i necessari presupposti, se non, addirittura, variabili del tutto estranee. In primo luogo, la destinazione, la funzione e lo scopo della valutazione e della selezione delle informazioni. L' esperienza statunitense è limitata ad un momento particolare del procedimento penale, necessariamente circoscritto e proprio del sistema processuale del *sentencing*, riservato al momento di commisurazione della pena. Per la precisione, una componente del processo penale che esprime un principio di carattere sistematico: la pena non è determinata sulla base della sola colpevolezza, ma è informata anche alla vita e alle caratteristiche dell'imputato. Se l'esperienza statunitense in questo senso vale a qualcosa, lungi dal voler intraprendere uno sterile tentativo di comparazione, essa fornisce quantomeno le basi per una valida riflessione di carattere metodologico.

Il principale assunto del caso *Loomis* risiede nella determinazione del dato statistico come elemento del patrimonio di conoscenze del giudice. Una componente non assoluta ed anzi da

[30] State v. Loomis, 881 N.W.2d par. 768.
[31] State v. Loomis, 881 N.W.2d par. 769.
[32] State v. Loomis, 881 N.W.2d par. 15.

circoscrivere ad una riflessione di opportunità al caso concreto. A questo si aggiunge la peculiarità propria degli algoritmi predittivi a fornire una soluzione non motivata, là dove vincolata ai limiti del brevetto, e potenzialmente discriminatoria, caratteristica tale da renderne l'utilizzo alquanto problematico.

Dall'esperienza statunitense si ricava ugualmente la necessità di limitare l'ambito di operatività dell'algoritmo alla scopo per cui è stato progettato e che tale attività sia garantita da un controllo non solo all'avanguardia ma costante, tale da uniformare il giudizio ai progressi tecnologici quanto alle evenienze del caso. Non si tratta solo della 'migliore scienza ed esperienza' in materia di programmazione di *software*, per riprendere un lessico, per altri versi, direttamente connesso alla materia degli algoritmi predittivi, ma di individuare e mantenere una *coerenza* costante tra il procedimento utilizzato ed il suo scopo. Si tratta di compiere, in questo senso, un adeguamento particolare, *granulare*[33] che sia in grado di adattare l'algoritmo ai tempi, agli scopi ed alle circostanze del suo impiego.

I procedimenti decisori in materia di recidiva e determinazione della pena non sono gli unici potenzialmente interessati dall'impiego di algoritmi predittivi. È facile intuire l'utilità di un efficiente meccanismo di elaborazione di dati statistico-probabilistici nell'ambito dell'accertamento del nesso causale. Anche in questo caso, è stato osservato, gli assunti di carattere generale formulati in materia di algoritmi predittivi sembrano riflettere un'eco lontana: «sicuramente, un dato statistico particolarmente prossimo alla certezza (pari al 100% di osservazione di quell'evento in determinate circostanze) fornirà all'inferenza sul fatto da provare una «base oggettiva», ma non colmerà di certo da solo quel *quid pluris* richiesto per superare, nel caso di specie, la soglia epistemica del ragionevole dubbio»[34].

Quello che si potrebbe definire un problema di *input* si rivela, principalmente, un problema di significato. In quanto tale, non è peregrino che gli studi di perfezionamento tecnologico in materia si rivolgano anche e soprattutto al legislatore, al *policymaker*[35] allo scopo di ottimizzare la funzionalizzazione degli algoritmi non solo in termini tecnologici, ma anche "politici", trattandosi di attività che richiedono un indirizzo specifico e selettivo. In ordine alla necessità di ridurre al minimo le variabili di "disturbo" all'interno dell'algoritmo decisorio, di rendere la valutazione scevra da pregiudizi e informazioni inconferenti rispetto allo scopo, non è necessario soltanto un miglioramento delle tecniche di programmazione dei software, ma anche e soprattutto una maggiore consapevolezza dei limiti di un calcolo statistico – probabilistico ai fini di una valutazione e dunque una conoscenza concreta del significato e dei contenuti attributi alle informazioni conferite alla macchina[36].

Sembra che l'esperienza degli algoritmi predittivi, fosse anche destinata a risolversi in uno sforzo di immaginazione, suggerisca una definizione di *precisione* del giudizio che non è semplificazione ed economicità, ma, prima di tutto, consapevolezza dei significati, necessità di definire e circoscrivere l'oggetto e lo scopo del giudizio. Si tratta di una dinamica che appartiene al diritto ed alla norma penale, prima che alla dimensione processuale. Una simile evidenza si palesa nel momento in cui s'immagina l'impiego di meccanismi decisionali automatizzati al fine di prevedere intere sentenze[37]. Del resto, può essere oggetto di un calcolo statistico – computazionale un insieme di dati qualsiasi, derivino questi da un casellario giudiziale, una raccolta di leggi statistiche piuttosto che massime giurisprudenziali o sentenze avanti il medesimo oggetto, capo di imputazione, legge applicabile. In tal caso, l'algoritmo predittivo non fornirebbe altro che la risultante di un processo statistico – probabilistico in grado di individuare un dato livello di pericolosità sociale, il grado di probabilità di verificarsi di un evento e finanche la legge applicabile al caso concreto ed, in mancanza di questa, il precedente rilevante ai fini di una decisione.

Quest'ultima ipotesi, non peregrina tra gli studiosi di calcolo computazionale applicato al diritto[38], ne rivela un chiaro limite. La scelta del precedente rilevante e, precisamente, l'insieme complesso del diritto vivente di matrice giurisprudenziale segna il momento in cui, inequivocabilmente, la parola del giudice rivela la propria appartenenza ad un linguaggio di tipo *valutativo* e *performativo*, ben lungi dall'essere limitato a risultanze computazionali e probabi-

[33] Kleinberg *et al.* (2018), pp. 237–293; Kehl *et al.* (2017), p. 33.
[34] Costanzi (2018), p. 183.
[35] Michael *et al.* (2016) p. 180.
[36] Kehl *et al.* (2017), 34.
[37] Aletras *et al.* (2016), p. 300.
[38] Hildebrandt (2018), pp. 12-35; Alarie (2016), pp. 443–55.

listiche. Si tratta di un fenomeno che caratterizza il complesso degli ordinamenti di *common law* e che da tempo ha visto, nel nostro ordinamento, la "supplenza giudiziaria" divenire una «categoria dello spirito legislativo»[39].

In tal evenienza, la pretesa obiettività di un linguaggio statistico – probabilistico e delle sue risultanti, di fronte all'incertezza dell'interpretazione, propria anche delle azioni umane, degli eventi e delle loro ragioni, non resterebbe altro che l'ennesima variabile indeterminata. La sfida degli algoritmi predittivi e dei processi decisionali automatizzati presenta agli occhi del giurista vasti territori inesplorati, davanti ai quali è possibile, tuttavia, distinguere i confini di *habitat* familiari. Le scienze matematiche hanno da tempo conosciuto il potere delle statistica nelle scienze sociali, che in parte esprime un tratto significativo proprio del linguaggio giuridico, in larga misura indipendente dalla sua applicazione[40], che non si limita a descrivere la realtà, ma arriva ad intervenire su di essa per esercitarvi un potere: «le leggi statistiche delle scienze sociali vedono accresciuto il loro ufficio, che non è soltanto quello di stabilire empiricamente la risultante di un gran numero di cause sconosciute, ma soprattutto di dare della realtà una testimonianza immediata e concreta. La cui interpretazione richiede un'arte speciale, non ultimo sussidio dell'arte di governo»[41].

Bibliografia finale

Bogost, Ian (Jan. 15, 2015), *The Cathedral of Computation*, (The Atlantic, http://www.theatlantic.com/technology/archive/2015/01/the-cathedral-of-computation/384300/).

Sheppard, Brian (2015): "Incomplete Innovation and the Premature Disruption of Legal Services", *Michigan State Law Review* , 5, pp. 1790 – 1910.

Casey, Anthony e Niblett, Anthony (2016): "Self- Driving Laws", *University Of Toronto Law Journal*, 66, 4, 2016, pp. 429-42;

Alarie, Benjamin (2016): "The Path Of The Law: Towards Legal Singularity", *University Of Toronto Law Journal*, 1, 2016, pp. 443–55

Susskind, Richard (2010) *The End Of Lawyers? Rethinking The Nature Of Legal Services* (Oxford, Oxford University Press)

Katz, Daniel Martin (2013): "Quantitative Legal Prediction – Or – How I Learned To Stop Worrying And Start Preparing For The Data Driven Future Of The Legal Services Industry", *Emory Law Journal*, 62, pp. 142-182.

Hildebrandt, Mireille (2018) "Law As Computation In The Era Of Artificial Legal Intelligence. Speaking Law To The Power Of Statistics", *University Of Toronto Law Journal*,68, 1, pp. 12-35;

Oswald, Marion - Grace Jamie - Urwin, Sheena - Barnes, Geoffrey (2018): "Algorithmic Risk Assessment Policing Models: Lessons From The Durham Hart Model And 'Experimental' Proportionality", *Information & Communications Technology Law*, 27:2, pp. 223-250;

Urwin, Sheena (2017): *Algorithmic Forecasting Of Offender Dangerousness For Police Custody Officers: An Assessment Of Accuracy For The Durham Constabulary Model*, Master's Thesis, University Of Cambridge.

Council Of Europe Study, *Algorithms And Human Rights – Study On The Human Rights Dimension Of Automated Data Processingtechniques And Possible Regulatory Implications*, 2017.

[39] Padovani (1992), pp. 419 ss.
[40] Hildebrandt (2018), p. 17.
[41] Majorana(1942), p. 66.

Montedoro, Giancarlo (20 Marzo 2018) intervento al Convegno "Giustizia e Intelligenza Artificiale", incontro organizzato nell'ambito dei "Martedì dell'associazione Vittorio Bachelet".

Angwin, Julia Et Al. (23 Maggio 2016) "Machine Bias: There's Software Used Across The Country To Predict Future Criminals. And It's Biased Against Blacks", (Pro Propublica, https://www.propublica.org/article/machine-bi-as-risk-assessments-in-criminal-sentencing).

Stith, Jane - Cabranes, Josè A. (1998): *Fear Of Judging. Sentencing Guidelines In The Federal Courts*, (Chicagom The University Of Chicago Press).

J. L. Koepke – D. G. Robinson, *Danger Ahead: Risk Assessment And The Future Of Bail Reform*, In *Washington Law Review*, Vol. 93, 2018 .

Kehl, Danielle - Guo, Priscilla and Kessler, Samuel (2017): "Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing". *Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School.*

Dolcini, Emilio (1984): *La Commisurazione Della Pena Tra Teoria E Prassi* (Padova, CEDAM)

Conso, Giovanni (1968): "Prime considerazioni sulla possibilità di dividere il processo penale in due fasi, *Rivista italiana di diritto e procedura penale,* pp. 706-712;

Zimring, Franklin (1977): "Making The Punishment Fit The Crime: A Consumers' Guide To Sentencing Reform", *University Of Chicago Law Occasional Paper*, 12, 1977, pp. 4-20.

Mannozzi, Grazia (1991) *Sentencing*, (Voce) In *Digesto Delle Discipline Penalistiche*, Vol. XIII (Torino, Utet) 1991, 151 Ss.

Hentig, Hans V. (1933-1934): "The Clinical Method In Teaching Criminal Law", *24 Am. Inst. Crim. L. & Criminology,* pp. 1081-87.

Starr, Sonja B. (2013): "Evidence-Based Sentencing And The Scientific Rationalization Of Discrimination", *Stanford Law Review*, 66, 4, 803.

Eaglin, Jessica (2017): "Constructing Recidivism Risk", *Emory L.J.* 59, 2017, pp. 67-90.

Kleinberg, Jon - Lakkaraju, Himabindu - Leskovec, Jure - Ludwig, Jens - Mullainathan, Sendhil (2018): "Human Decisions And Machine Predictions", *The Quarterly Journal Of Economics* 133, 1, 2018, pp. 237–293.

Costanzi, Claudio (2018) "La matematica del processo: oltre le colonne d'ercole della giustizia penale", *Questione Giustizia.*

Michael, Luca – Kleinberg, Jon – Mullainathan, Sendhil (2016): "Algorithms Need Managers, Too", *Harvard Business Review*, Vol. 94, Nº 1

Algoritmi predittivi e discrezionalità del giudice: una nuova sfida per la giustizia penale

Algoritmos predictivos y discrecionalidad del juez: un nuevo desafío para la justicia penal

Predictive Algorithms and Judicial Discretion: a New Challenge for Criminal Justice

Lucia Maldonato
Dottoressa di ricerca presso l'Università Cattolica di Milano
lucia.maldonato@unicatt.it

Intelligenza artificiale | Inteligencia artificial | Artificial Intelligence

Abstracts

Negli Stati Uniti gli algoritmi predittivi del rischio di recidiva si sono imposti nell'ordinario svolgersi delle dinamiche processuali, sia nella fase che precede il giudizio, sia al momento del *sentencing*. Il contributo si propone di analizzare la struttura e il procedimento di formazione degli strumenti algoritmici di *risk assessment*, mettendo in evidenza le criticità che connotano tali *software*. Si insisterà in particolare sull'ontologica inaccessibilità dello strumento, che ad oggi opera come una *black box*, rendendo impossibile qualsiasi controllo sulle sue risultanze da parte delle difese, ma anche sul fatto che i risultati dell'algoritmo, in ragione della loro patina di oggettività, potrebbero condizionare il giudice, col pericolo che lo stesso possa non apprezzare adeguatamente le evidenze fattuali, per concentrarsi sul tipo di autore. Le nuove tecnologie di intelligenza artificiale, però, se adeguatamente comprese e utilizzate, potrebbero trovare spazi di operatività anche nel nostro sistema e in particolare al momento della determinazione del *contenuto* della sanzione penale, che potrebbe finalmente essere intesa come un progetto e non come mero momento retributivo

En los Estados Unidos los algoritmos predictivos del riesgo de reincidencia son utilizados en el proceso, tanto en la fase que precede a la sentencia como en la determinación de la pena. El presente trabajo tiene por finalidad analizar la estructura de los algoritmos predictivos del riesgo de reincidencia, destacando los problemas existentes a su respecto. Se pone especial énfasis en la inaccesibilidad de los instrumentos, los cuales usualmente operan como una caja negra, así como en el hecho de que el resultado de que tales algoritmos puedan condicionar la decisión del juez. No obstante, las nuevas tecnologías de inteligencia artificial, si son correctamente entendidos y aplicados, podrían encontrar cabida en nuestro sistema, en particular al momento de la determinación de la pena, la cual podría ser entendido como un proyecto y no como un mero momento retributivo.

In the United States predictive algorithms of recidivism are used in the ordinary unfolding of trials, not only in the pre-verdict phase, but also in sentencing. This paper aims to analyze algorithmic risk assessment tools' structure, highlighting all the critical issues that connote these softwares. Particular emphasis will be placed on the inaccessibility of the instrument, which currently operates as a black box, but also on the fact that the outcome of such algorithms could bias the judge's decision. Nevertheless, new artificial intelligence technologies, if properly understood and applied, could find room also in our system and in particular at the time of determining the content of the sanction, which could finally be understood as a project and not as mere retribution.

Sommario

1. *Loading*… La giustizia digitale.

La rivoluzione derivante dall'imporsi degli strumenti digitali e la trasformazione radicale delle modalità di comunicazione ha ormai assunto un carattere trasversale, lambendo tutti i settori dell'attività umana, non ultimo il diritto[1].

La giustizia digitale[2] è infatti un fenomeno che va al di là della cosidetta *legaltech*, settore che riguarda le applicazioni tecniche in ambito giuridico[3], oltre la tecnologia *blockchain*[4] o degli *smart contracts*[5], atteggiandosi piuttosto, come si vedrà, alla stregua di una «fonte alternativa della normatività»[6]. La giustizia digitale, o giustizia predittiva[7], intesa come capacità delle nuove tecnologie di intelligenza artificiale[8] (da questo momento AI) di sostituirsi agli attori processuali nell'amministrazione dello *ius dicere* sta ormai rivendicando sempre più il proprio spazio, imponendosi per la sua efficienza all'attenzione del giurista, che deve comprendere e affrontare il linguaggio delle intelligenze artificiali, il linguaggio binario.

L'idea di un algoritmo che possa soppiantare l'uomo al momento della decisione - anche ove ciò comporti la produzione di conseguenze nella sfera giuridica di un altro soggetto - non è più soltanto il portato della fantasiosa immaginazione di scrittori e registi[9], ma una realtà con la quale è diventato obbligatorio confrontarsi, specie a seguito dell'emanazione del Regolamento europeo in materia di protezione dei dati personali (GDPR). L'art.15 della Direttiva

[1] In argomento si vedano le riflessioni di Garapon, Lassegue (2018), p. 12. In tema, nella dottrina statunitense, si v. Chander (2017), p. 1023 ss., ove l'A. evidenzia come il processo di *decision making* sia solo marginalmente riservato all'uomo, essendosi ormai imposti in ogni settore i procedimenti decisionali computerizzati, dal credito, all'investimento di denaro, agli incontri interpersonali.

[2] Per un interessante studio su questo tema si rinvia a Garapon, Lassegue (2018), *passim*.

[3] Si pensi alla rivoluzione del processo civile telematico e alla progressiva affermazione del processo penale telematico.

[4] Con il termine "*blockchain*" (letteralmente "catena di blocchi") si indica, in estrema sintesi, un vero e proprio registro pubblico condiviso, un libro contabile che si aggiorna automaticamente su ciascuno dei nodi che partecipano alla rete. Un'architettura *blockchain* definisce un deposito di dati distribuito, costituito da una lista di record in continua crescita resistente a modifiche e revisioni, anche da parte degli operatori dei nodi (computer) su cui risiede il deposito di dati. I dati sono così sicuri anche in presenza di partecipanti non affidabili in rete.

[5] Su questi profili, cfr. Crisci (2018), p. 1799.

[6] Per un interessante inquadramento della questione, cfr. Garapon, Lassegue (2018), p. 13 ss.

[7] Garapon, Lassegue (2018), p. 219. La giustizia predittiva individua *stricto sensu* la capacità di una macchina di individuare le norme pertinenti per trattare una determinata vicenda, di metterla in connessione con le caratteristiche proprie del fatto e di anticipare le decisioni che potranno intervenire. L'espressione ha oggi un carattere maggiormente generico e fa riferimento a tutte le innovazioni tecnologiche che avvengono nel dominio del diritto. La giustizia predittiva non vuole soppiantare il diritto ma migliorarlo e renderlo più prevedibile. Sull'argomento v. anche Viola (2018), p. 1, «Per giustizia predittiva deve intendersi la possibilità di prevedere l'esito di un giudizio tramite alcuni calcoli, non si tratta di predire tramite formule magiche, ma di prevedere la probabile sentenza, relativa ad uno specifico caso, attraverso l'ausilio di algoritmi. Il diritto può essere costruito come una scienza, che trova la sua principale ragione giustificativa nella misura in cui è garanzia di certezza: il diritto nasce per attribuire certezza alle relazioni umane, tramite una complessa attribuzione di diritti e doveri». Secondo l'A., dunque, la prevedibilità delle decisioni è in connessione immediata con il carattere di certezza del diritto: l'interpretazione delle norme potrà dunque operarsi anche con linguaggio binario, tipico delle intelligenze artificiali. Diversi e interessantissimi sono stati gli studi in materia di giustizia predittiva. In particolare L'University College di Londra e l'Università di Sheffield, nel 2017, hanno condotto uno studio a livello testuale su 586 casi giudiziari decisi dalla Corte europea dei diritti dell'uomo in materia di giusto processo, privacy e trattamenti disumani. L'algoritmo ha individuato fatti, circostanze ricorrenti, frasi più frequentemente rinvenibili nei casi di violazione dei diritti fondamentali e ha predetto il verdetto corretto nel 79% dei casi. Su questo argomento, cfr. Barbaro (2018), p. 191, in part. nota 6. Sempre nel 2017 la piattaforma internet Case Crunch ha condotto la prima competizione tra intelligenze artificiali (AI) e avvocati. AI ha individuato il verdetto corretto con un'accuratezza del 86,6% contro il 62,3% dei legali su casi relativi a proprietà intellettuale discussi davanti al Financial Ombudsman Service. Ancora, sul concetto di giustizia predittiva, cfr. Castelli, Piana (2018), p. 154.

[8] L'intelligenza artificiale può definirsi come «l'insieme di studi e tecniche che tendono alla realizzazione di macchine, specialmente calcolatori elettronici, in grado di risolvere problemi e riprodurre attività proprie dell'intelligenza umana», così De Mauro (2000).

[9] Si pensi ad esempio al romanzo di Philip K. Dick, *The Minority Report*, Pantheon Books, New York, 2002 da cui è stato tratto l'omonimo celebre lungometraggio di S. Spielberg. Romanzo e film raccontano la storia di John Anderton, responsabile della sezione *Precrimine* della polizia della città di Washington. Tale sezione di polizia, basandosi sulle premonizioni di tre individui dotati di poteri extrasensoriali di precognizione amplificati, detti *Precog*, è in grado di impedire gli omicidi prima che essi avvengano e ad arrestare i potenziali "colpevoli". In questo modo non viene punito il fatto (che non avviene), bensì l'intenzione di compierlo e chi porterebbe a concretizzarlo.

95/46/CE, confluito nell'art. 22 del nuovo Regolamento 2016/679/UE[10], stabilisce che ogni persona ha il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o abbia conseguenze significative nei suoi confronti, fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità.

In relazione al particolare profilo del trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati, il Parlamento Europeo e il Consiglio hanno adottato la Direttiva 2016/680/UE, che, all'art. 11, riproduce i contenuti dell'art 22 del GDPR. L'Italia ha dato attuazione alla predetta Direttiva con il Decreto legislativo 18 maggio 2018 n. 51, ove all'art. 8 si stabilisce che "Sono vietate le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge. Le disposizioni di legge devono prevedere garanzie adeguate per i diritti e le libertà dell'interessato. In ogni caso è garantito il diritto di ottenere l'intervento umano da parte del titolare del trattamento".

Se l'Unione europea ha ritenuto di dover regolamentare il trattamento automatizzato di dati, imponendo un divieto tanto stringente per la loro utilizzazione in sede processuale[11], lo studioso attento non potrà fare a meno di confrontarsi con la struttura e le problematiche che tali nuovi strumenti pongono, anche rispetto al sistema della giustizia penale. In tale prospettiva, pare interessante muovere dall'esperienza di quell'ordinamento che, ormai da decenni, utilizza gli algoritmi nel processo penale, l'ordinamento statunitense.

2. Gli algoritmi predittivi e un viaggio oltreoceano: lo strano caso di Eric Loomis.

L'utilizzo di algoritmi che processano *Big Data* è diventata una prassi sempre più comune per il sistema penale degli Stati Uniti, laddove tali *software* vengono utilizzati sia per fornire indicazioni su una più efficiente allocazione delle risorse di polizia, sia per orientare gli sforzi dell'ordinamento, così da intervenire sugli individui maggiormente esposti alla possibilità di essere coinvolti in attività criminali, sia come strumento riservato ai giudici per prendere decisioni nella fase preliminare del giudizio, ad esempio per la determinazione dell'ammontare della cauzione o per le valutazioni circa la concessione del *parole*[12].

Non è trascorso molto tempo, però, perché gli algoritmi si imponessero all'attenzione del giudice anche nella fase per questi più impegnativa e gravida di pressioni, la fase della commisurazione della pena (*sentencing*). È in tale momento che i giudici sono tenuti ad apprezzare non soltanto la pena adeguata al fatto perpetrato ma anche il rischio di recidiva, operando una prognosi sulla probabilità che quest'ultimo incorra nuovamente nella commissione di un fatto di reato. Può dirsi pertanto che, nelle Corti statunitensi, si sta progressivamente affermando un originale approccio data-centrico alla prognosi di recidiva che il giudice è tenuto a formulare, attraverso l'utilizzazione di strumenti pre-formati di *risk assessment*[13]: gli algoritmi predittivi del rischio di recidiva.

Uno dei primi (e più interessanti) casi in cui una Corte, nella specie quella del Wisconsin, si è avvalsa dell'utilizzo di algoritmi predittivi è certamente quello di Eric Loomis[14]. Nel 2013

[10] Anche la Commissione europea sull'efficacia della giustizia (Cepej) si è occupata del tema, redigendo una «Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziari», adottata alla sessione plenaria della Cepej del 3-4 dicembre 2018. Primo strumento europeo in materia, la Carta etica enuncia principi sostanziali e metodologici applicabili all'analisi e al trattamento delle decisioni giudiziarie e vuole essere un punto di riferimento per l'attività di soggetti privati e pubblici attivi in questo settore, sia per lo sviluppo concreto di applicazioni di intelligenza artificiale sia per l'elaborazione di politiche pubbliche riguardanti l'integrazione di tali applicazioni nel sistema giudiziario. In particolare la Carta etica si ispira ai principi del rispetto dei diritti dell'uomo, della non discriminazione e della trasparenza delle metodologie di costruzione dei *software*, che devono poter essere verificate da soggetti terzi e indipendenti. Su questi profili, cfr. Barbaro (2018), pp. 189 ss.; Gialuz (2019), pp. 12-15.

[11] Sull'utilizzo degli algoritmi nel procedimento amministrativo, limitatamente all'ipotesi di atto vincolato (quantomeno allo stato attuale), si v. Viola (2018), pp. 1588 ss., in particolare pp. 1601 ss.

[12] L'istituto del *parole*, assimilabile alla liberazione condizionale, consiste nel temporaneo rilascio di un prigioniero che consente di adempiere determinate prescrizioni prima di aver scontato la pena. In argomento si veda Joyce (2018), p. 82 ss.

[13] Tali strumenti potrebbero costituire una potenziale soluzione al peso morale gravante sul giudice al momento della decisione, sul punto v. *Harvard L. Rev.* (2017), p. 1530 ss.

[14] *State v. Loomis,* 881 N.W. 2d 749 (Wis. 2016). La Corte del Wisconsin si era già pronunciata su un altro caso utilizzando l'algoritmo COMPAS. Si tratta del caso di Paul Zilly, imputato per diversi episodi di furto. Zilly aveva inizialmente patteggiato la pena di un anno di carcere in una prigione della contea seguita da un periodo di controllo. L'imputato però era stato condannato a due anni di *prison*: i giudici

Loomis era stato tratto a giudizio per rispondere di due reati che nel nostro Paese corrispondono a ricettazione (di un'automobile) e resistenza a pubblico ufficiale. Nella fase precedente all'udienza di *sentencing* l'ufficiale del *Wisconsin Department Of Correction* aveva prodotto un *report* con investigazioni preliminari (PSI[15]) che, oltre a fornire alla Corte informazioni sull'imputato, includeva anche una valutazione del rischio di recidiva formulata da COMPAS, l'algoritmo predittivo che, sulla base dei dati inseriti nel sistema e di un questionario di 137 domande che si sottopone al reo, attribuisce allo stesso uno *score*, un punteggio che esprime il rischio di ricaduta nella commissione di reati. COMPAS è però un algoritmo proprietario, coperto dal *trade secret*; conseguentemente, alla Corte era stato fornito il nudo dato matematico espressivo del rischio di recidiva, senza alcuna delucidazione circa i meccanismi di funzionamento del *software*. La Corte, tenendo in considerazione anche le risultanze offerte da COMPAS, aveva condannato Loomis a sei anni di reclusione e cinque anni di *extended supervision*[16].

Il condannato aveva a quel punto proposto una mozione per un *post-conviction relief*, lamentando la violazione del diritto al giusto processo; Loomis asseriva infatti che era stato frustrato il suo diritto ad avere una sentenza individualizzata e ad esser giudicato sulla base di informazioni accurate, poiché COMPAS fornisce dati rilevanti solo per gruppi specifici, con un meccanismo di funzionamento che non poteva essere controllato in alcun modo dalle difese[17].

Nel luglio 2016 la Corte Suprema del Wisconsin, pronunciandosi sul ricorso di Loomis, aveva dichiarato, all'unanimità, la legittimità dell'uso giudiziario di algoritmi che misurano il rischio di recidiva specificando, tuttavia, che lo strumento non può essere l'unico elemento su cui si fonda una pronuncia di condanna[18].

La vicenda Loomis solleva una serie di profili che evidenziano le problematicità connesse all'utilizzo dell'algoritmo: dalla tecnica di costruzione del *software*, che si presta a riprodurre le discriminazioni verso le minoranze etniche anche nei punteggi emessi all'esito del calcolo, al difetto di trasparenza dello stesso; dal potenziale condizionamento che un *software* può esercitare nei confronti dell'organo giudicante, al problema del deficit di controllabilità di un sistema coperto da diritto d'autore. Di queste problematicità occorre occuparsi, al fine di corroborare la valutazione degli eventuali possibili spazi all'interno del nostro sistema per l'utilizzo di tali strumenti.

3. Il "cuore" dell'algoritmo: base di calcolo e discrezionalità del programmatore.

È necessario preliminarmente verificare più da vicino le modalità attraverso cui gli sviluppatori dello strumento algoritmico di *risk assessment* procedono alla sua costruzione, tenendo sempre ben presente che lo stesso costituisce una *black-box*[19], un sistema cioè operante con connessioni tutt'oggi non spiegabili sul piano tecnico, che, a seguito del calcolo, mette a disposizione un risultato espresso in termini numerici, senza però fornire alcuna indicazione sulla metodologia utilizzata per addivenire a tale dato.

Un algoritmo è infatti una sequenza di istruzioni in base alle quali il calcolatore elabora un processo, che si struttura come un susseguirsi di operazioni che forniscono un risultato concreto, reale e virtualmente utile; l'informazione finale generata dal calcolo costituisce il prodotto dell'incrocio tra le diverse categorie di dati inseriti nella base dell'algoritmo.

In particolare, gli algoritmi che stimano il rischio di recidiva si fondano sull'analisi attuariale o statistica delle osservazioni operate su dati relativi al comportamento degli individui

avevano considerato i risultati dell'algoritmo COMPAS, che assegnava a Zilly un elevatissimo *risk score* per futuri crimini violenti. Il giudice Babler, estensore della sentenza, si era così espresso: «*Had I not had the COMPAS, I believe it would likely be that I would had given one year, six months*». In argomento, v. anche. Carlson (2017), p. 319-320.

[15] *Presentencing Investigation Reports*.

[16] In argomento si rinvia alle considerazioni di Carlson (2017), pp. 319 ss. ove afferma che nei casi Zilly e Loomis, i giudici del Wisconsin hanno fondato la propria decisione sui punteggi di COMPAS, emanando una sentenza sfavorevole per l'imputato.

[17] *State v. Loomis*, at. 757.

[18] Il giudice Bradley, estensore della sentenza, riteneva che il problema dell'individualizzazione del giudizio fosse meno grave di quanto prospettato dal ricorrente Loomis in quanto le Corti continuano a possedere quella discrezionalità e quelle informazioni necessarie a discostarsi dalle risultanze numeriche, quando ciò sia necessario. Sul punto v. *Harvard L. Rev.* (2017), 1530.

[19] Sottolinea questo aspetto Gaboriau (2018), p. 209.

precedentemente arrestati o condannati. Gli strumenti classificano un imputato in base a una serie di fattori identificativi, che sono in correlazione con il verificarsi di comportamenti criminali specifici. Molti di questi fattori non si riferiscono al reato di cui all'imputazione o alla storia criminale dell'agente. Se utilizzato per la condanna, il risultato dello strumento stima la probabilità che un imputato si impegni in un comportamento criminale *qualsiasi*, in un *futuro più o meno prossimo*.

Alla luce di tali considerazioni introduttive è evidente la valenza euristica dello strumento algoritmico, in grado di incamerare un'enorme quantità di dati e di effettuare predizioni che, almeno all'apparenza, sono molto più accurate, efficienti e *fair* di quelle operate dal giudice persona fisica. L'algoritmo non è altro che un calcolo, seppur complicatissimo, e nella sua asetticità potrebbe apparire più affidabile di quanto possa essere il giudizio umano[20].

D'altro canto, le modalità attraverso le quali tali *software* vengono costruiti hanno enorme rilievo rispetto alle "verità" di cui sono realmente portatori i risultati del calcolo operato. La dottrina d'oltreoceano che più da vicino si è occupata del tema[21] ha evidenziato che gli sviluppatori degli strumenti in esame compiono inevitabilmente una serie di assunzioni implicite nel corso della progettazione; come si vedrà, tali assunzioni sottendono giudizi aventi ad oggetto sia questioni di politica criminale sia questioni relative alle circostanze valutabili in sede di giudizio (ad es. la personalità del reo, il suo carattere, le sue inclinazioni).

In una prima fase, che potremmo definire di costruzione vera e propria, i programmatori dell'algoritmo devono individuare i dati da raccogliere e la fonte cui attingere, che può essere tra le più diverse: si può condurre uno studio su persone selezionate, ottenere le informazioni da agenzie governative o semplicemente individuare i dati da informazioni già disponibili al pubblico per altri scopi. È stato osservato che gli sviluppatori necessitano di osservazioni sufficientemente varie per costruire un *data-set* che possa fornire risultati attendibili. A tale fine, le osservazioni non potranno essere effettuate su comportamenti oltremodo specifici, poiché troppo esigue sarebbero le informazioni a disposizione e troppo alto il rischio da sopportare per la società in caso di falso negativo[22]. Per ovviare a quest'ultimo inconveniente i programmatori, ordinariamente, scelgono quale evento finale oggetto della predizione algoritmica, un evento generico, tale da incrementare il *data-set* di base. In altre parole gli stessi scelgono di semplificare al massimo la domanda predittiva posta alla base dell'algoritmo: gli si domanderà di effettuare una prognosi su eventi generici, come ad esempio tutti i reati commessi con violenza o anche, indifferentemente, tutti i delitti e le contravvenzioni. Il rischio, però, è che i programmatori possano manipolare i dati aggregando distinte tipologie di offese per arricchire quanto più possibile la base informativa.

A seguito della formazione del *data-set* è necessario poi definire la domanda da porre all'algoritmo in termini misurabili; segnatamente gli sviluppatori dovranno definire cosa vogliono intendere per rischio di recidiva agganciandolo ad un fenomeno concretamente rilevabile, come può essere un nuovo arresto, una nuova condanna, ovvero la semplice violazione delle prescrizioni imposte a seguito della concessione del *parole*[23]. Anche in questo caso è facile osservare come ciò configuri un nuovo giudizio a carattere normativo, avente ad oggetto un elemento di estremo rilievo: il comportamento criminale che dovrebbe inverare il rischio di recidiva.

Uno dei comportamenti più frequenti tra quelli assunti dagli osservatori quale evento espressivo della recidiva è proprio l'arresto[24], poiché le informazioni sul numero e la frequenza

[20] Per una posizione di apertura rispetto all'utilizzo degli algoritmi in tutte le fasi del processo penale si rinvia a Simmons (2018), pp. 573 ss. L'Autore ritiene che, rendendo gli algoritmi trasparenti e migliorandoli in modo da rimuovere quei *biases* che inevitabilmente li connotano, gli stessi potrebbero essere un utile strumento per raggiungere risultati più efficienti. Simmons ritiene poi che l'utilizzo degli algoritmi potrà definitivamente imporsi guadagnando il supporto dell'opinione pubblica, supporto che potrà essere raggiunto solo se l'algoritmo stesso verrà percepito come giusto (*fair*). Secondo l'A. la percezione della *fairness* dello strumento incoraggia atteggiamenti di adesione ai precetti e dunque può sortire un effetto non indifferente in termini di prevenzione generale.

[21] Sul punto, v. Eaglin (2017), pp. 60 ss.

[22] In qualunque ambito in cui si presenti una decisione predittiva binaria (vero o falso), un falso negativo indica che è stata erroneamente segnalata come assente una caratteristica che in realtà è presente.

[23] Se si optasse per considerare tale accadimento come espressivo di recidiva allora nella base di calcolo entrerebbero anche tutte quelle violazioni solo formali delle prescrizioni imposte, come ad esempio un ritardo o un semplice difetto di comunicazione con l'incaricato della sorveglianza. È evidente che violazione tecnica o una contravvenzione non sono in alcun modo equiparabili alla commissione di un crimine violento.

[24] L'algoritmo VRAG assume quale fattore indicativo della recidiva ogni nuovo comportamento criminale anche se non sfocia in un arresto; l'algoritmo ORAS seleziona invece i dati circa gli arresti per qualsiasi violazione. Sulle diverse tipologie di algoritmi si rinvia a Eaglin (2017), p. 70 ss.; Singh *et al.* (2018), *passim*.

di questo sono generalmente di facile reperimento; il numero di arresti effettuati consente di creare in maniera accessibile, semplice e a costo zero una base informativa assai varia. Il punto verrà ripreso ma preme sin d'ora evidenziare che la scelta dell'arresto come fattore espressivo della recidiva si presta a far riprodurre nei risultati dell'algoritmo una diseguaglianza strutturale presente nella società e ormai accettata come normale[25]. È noto, infatti, che negli Stati Uniti gli arresti vengono effettuati in maniera sproporzionata nei confronti delle minoranze e, in particolare, nei confronti di uomini di colore. Tuttavia - seppur banale, è comunque necessario precisarlo - un contatto più frequente con le forze dell'ordine non significa necessariamente un rischio più elevato per la sicurezza pubblica; gran parte dei contatti tra polizia e appartenenti a minoranze etniche non dipende necessariamente da una loro maggiore propensione a commettere crimini, quanto da un controllo più stringente da parte delle forze dell'ordine stesse nei confronti di soggetti appartenenti a minoranze[26].

Tornando alle modalità di costruzione dell'algoritmo, concluso il primo *step* con l'immissione di dati e domande, si apre la seconda fase. Questa, composta da un momento valutativo e da un momento comunicativo, consiste nella decisione sulla porzione di rischio sopportabile dal contesto sociale di riferimento e nella comunicazione di tale risultato agli attori processuali. I risultati dell'intersecarsi delle informazioni presenti nel *data-set*, in buona sostanza, vengono trasferiti dagli sviluppatori in determinate categorie rappresentanti il rischio di recidiva, categorie che rappresentano il livello di rischio, da basso a elevato, in termini numerici o percentuali.

In tale fase, massima è la discrezionalità dei programmatori, che tracciano le linee di confine tra i differenti livelli di rischio a seconda della valutazione sul grado sopportabile in un determinato contesto sociale[27]. La differenza tra un soggetto catalogabile a rischio basso e uno classificabile a rischio medio o alto dipende da una valutazione del programmatore, completamente libera da vincoli su dove fissare i cosidetti punti di *cut-off*, i nodi di passaggio tra i diversi livelli di rischio.

La disamina della modalità ordinaria di costruzione dell'algoritmo che stima il rischio di recidiva rende evidente come il risultato prodotto dal sistema costituisca la rielaborazione delle informazioni contenute nel *data-set* iniziale a disposizione dei programmatori. È necessario tuttavia rilevare che le scelte rispetto alla collezione dei dati, segnatamente la fonte da cui reperirli, le modalità di raccolta e di composizione della base di informazioni sono intimamente connesse con il luogo fisico e l'ambiente socio-culturale da cui tali dati promanano. Proprio in ragione di ciò «i dati e i *data-set* non sono informazioni oggettive, bensì sono creazioni del

[25] Sottolinea tale profilo Carlson (2017), p. 319 ss. Più in generale su questo tema si rinvia alle riflessioni di Forza, Menegon, Rumiati (2017), p. 107 ss. ove si evidenzia come sia fisiologico costruire schemi mentali di valutazione della personalità individuale. Schemi analoghi sono prodotti per le valutazioni di gruppi, di abitanti di una località, di popoli e razze. A un gruppo, anche nella vicenda processuale, si associano determinate caratteristiche ed emozioni; tali rappresentazioni cognitive o impressioni di un gruppo sociale, tanto per gruppi quanto per singoli individui, vengono definiti dagli psicologi sociali come *stereotipi*. Il processo di categorizzazione sociale si attua quando determinati soggetti non vengono più valutati nella loro individualità ma come parte di un gruppo: l'appartenenza etnica e l'età sono basi evidenti. Gli psicologi sociali hanno distinto tre diverse tipologie di stereotipo, operanti su tre diversi livelli, pubblico, privato e implicito. Particolarmente interessanti sono gli stereotipi a livello implicito, costituiti da tutta quella serie di elementi, ormai acquisiti al patrimonio cognitivo, che operano come associazioni mentali e che finiscono per influire sui giudizi e sul modo di agire, senza che vi sia consapevolezza di tutto ciò, indipendentemente dal fatto che tali associazioni coincidano con i convincimenti consapevoli. È stato ad esempio dimostrato che gli stereotipi razziali vengono mantenuti anche quando gli stessi soggetti a livello cosciente non condividono i contenuti dello stereotipo, anzi si dicono contrari agli stessi. Vi sono numerose ricerche condotte attraverso il Test di associazione implicita (*Implicit Association Test,* IAT) che dimostrano la dimensione di tale fenomeno. Con lo IAT, somministrato attraverso un computer a un gruppo sperimentale, si invita il soggetto a rispondere attraverso la pressione di due pulsanti associati a due categorie di risposta, *sì e no*. Più veloce è la risposta positiva o negativa di fronte allo stimolo (parola o immagine), maggiore è considerato il legame tra un concetto e un attributo. Una persona bianca, di fronte al concetto "persona di colore" è portata a rispondere in tempi più veloci a domande su attributi quali pigrizia, ostilità o attitudini atletiche. Allo stesso modo, l'attivazione del concetto "persona di pelle bianca" porta i soggetti di colore a dare risposte più rapide su quesiti imperniati su connotazioni correlate quali convenzionalità, ambizione, materialismo. Tali dati sono stati confermati dall'utilizzo della risonanza magnetica funzionale (fMR). Ai partecipanti venivano mostrate fotografie di individui bianchi o di colore, mentre si trovavano all'interno dello *scanner* di un dispositivo fMR. I dati di *imaging* hanno dimostrato che l'esposizione iniziale di tutte le facce produceva l'attivazione dell'amigdala, l'area cerebrale sottostante la corteccia cerebrale, coinvolta nel monitoraggio degli stimoli che producono emozioni e sensazioni di paura. A seguito degli esperimenti i ricercatori hanno constatato che i volti di persone appartenenti a gruppi razziali o etnici diversi dal proprio, in generale, vengono percepiti come minacciosi. Lo stereotipo razziale dunque costituisce un condizionamento inveterato, portato di processi adattivi millenari, condizionamento che sarà arduo superare.

[26] Cfr., sul punto, Chander (2017), p. 1028, che parla di *unconscious bias;* v. anche Carlson (2017), p. 97 ss., ove si afferma: «*Using arrest as the measure of recidivism makes it impossible for black defendants not to be classified as high risk with more frequency given that arrest rates differ by race*». Su questi temi si rinvia a Forti (2000), p. 113 ss.

[27] Secondo Eaglin (2017), p. 87, questa fase si configura come un "*highly subjective, policy-oriented process*". Sul processo attraverso cui si addiviene a fissare il *cutting point* si rinvia a Brennan, Dieterich (2018), pp. 59 ss.

design umano»[28], raccontano la storia e le caratteristiche del posto dal quale sono tratti[29].

Se quanto appena esposto è vero, allora non può non concordarsi con quella dottrina d'oltreoceano che rimarca come la reale questione circa l'utilizzo dell'intelligenza artificiale in sede processuale non sia solo (e non tanto) la non conoscibilità del modo di operare della *black box* algoritmica, quanto il fatto che è la realtà sintetizzata dai dati raccolti ad essere già compromessa da false percezioni, da *biases* che portano, tra l'altro, a discriminare le minoranze razziali e di genere[30]. A tale ultimo proposito pare importante chiarire sin d'ora che i *data-set* sono composti da dati già errati al momento della selezione, in quanto, come già in parte anticipato, riflettono pregiudizi nei confronti delle minoranze. Il *bias* di cui soffre l'algoritmo è dunque espressione di un più diffuso problema culturale e fare affidamento sugli *scores* dallo stesso prodotti potrebbe rafforzare discriminazioni e parzialità già esistenti e radicate nel contesto sociale[31].

Il pericolo di cui si è appena fatto cenno, poi, difficilmente potrà essere corretto e impone di non dimenticare che, almeno ad oggi, non è ancora possibile comprendere appieno il meccanismo di funzionamento del sistema complesso. Il problema dunque non può essere sbrigativamente accantonato, anche in considerazione del fatto che lo strumento algoritmico è in grado di automodificarsi e di estrarre informazioni anche non incluse all'interno del *data-set*[32]. È questo un fenomeno noto come *redundant encoding*, che aumenta in maniera esponenziale le criticità del sistema rispetto al rischio di rafforzare atteggiamenti discriminatori. Il *redundant encoding* è quel meccanismo per cui anche quando uno specifico *data marker* (ad esempio quello sulla razza del reo o sul genere sessuale) non è incluso tra le informazioni presenti, lo si potrà comunque ottenere attraverso il combinarsi di altri dati rilevanti. L'algoritmo dunque non è soltanto in grado di fornire risposte più velocemente dell'uomo ma pare in grado di prendere decisioni in totale autonomia, senza lasciare alcuna possibilità di comprendere il percorso decisionale attraverso cui si è addivenuti a un determinato risultato.

Non solo, ma una volta completata la costruzione dello strumento, lo stesso viene integrato con le informazioni tratte dal caso concreto, solitamente ottenute attraverso la somministrazione di un questionario[33].

In forza di quanto appena esposto, appare evidente quanto lo strumento dell'algoritmo costituisca ancora oggi un pianeta refrattario all'esplorazione e, ove mai dovesse porsi il problema di una sua utilizzazione anche nel processo penale italiano, enormi dovrebbero essere le cautele da apprestarsi. Pare infatti che i tradizionali rimedi costituiti dalla formazione della prova in contraddittorio e dall'obbligo di motivazione, da soli, non siano in grado di ostacolare la portata espansiva dei risultati dell'algoritmo, ciò in ragione di tre ordini di motivi: il difetto di scientificità del metodo di costruzione dello strumento, la potenziale lesione del diritto di difesa e il pericolo di condizionamento del libero convincimento dell'organo giudicante, che potrebbe essere portato ad abbandonare la valutazione del fatto per concentrarsi sul tipo di autore.

4. Tecnologia e metodo scientifico: un binomio non indissolubile. La macropsia dell'algoritmo.

È necessario, in primo luogo, considerare che l'impiego del mezzo tecnologico non è indefettibilmente connesso all'utilizzo di un metodo scientifico nella costruzione dello stesso[34].

[28] In tal senso, v. Eaglin (2017), p. 72.
[29] Su questo profilo v. Barbaro (2018), p. 194, che ritiene che l'algoritmo produca «effetti che si potrebbero qualificare deterministi, nel senso che inchiodano un individuo al destino di una comunità».
[30] Cfr., Chander (2017), p. 1028.
[31] In argomento si veda l'interessante riflessione di Simmons (2018), p. 574 ss., che ritiene possibile che lo sviluppo tecnologico possa consentire un sempre maggiore spazio di correzione degli algoritmi. In argomento v. anche Carlson (2017), p. 329 ss.
[32] Sulla capacità di automodificazione dell'algoritmo si rinvia alle relazioni del Dott. S. Suweis e del professor A. Simoncini, tenute presso l'Università Cattolica di Milano nel corso dell'incontro intitolato "*Rivoluzione digitale: che cosa sta accadendo?*", in data 27 novembre 2018. Sull'interessante questione del *machine learning* si rinvia a Crisci (2018), pp. 1795 ss.
[33] Lo strumento COMPAS in particolare prevede, oltre alla somministrazione di un questionario, anche l'effettuazione di un'intervista al reo, intervista che si compone di una serie di risposte aperte con le quali si intende garantire che il reo comprenda pienamente il significato e le finalità dell'utilizzo dello strumento algoritmico, Su questi aspetti si rinvia a Brennan, Dieterich (2018), p. 57.
[34] In tal senso, si rinvia a Costanzi (2018), p. 188, che evidenzia come i meccanismi di funzionamento degli algoritmi di *crime Analysis* facciano sorgere molteplici interrogativi sotto il profilo del rispetto dei principi sanciti dalla sentenza *Daubert* sulla verifica della scientificità

La veridicità di tale assunzione è lampante a un'osservazione più accurata dello strumento algoritmico[35].

Gli algoritmi che processano *Big Data* sono oggetto di studio della fisica dei sistemi complessi, disciplina che tenta di ricostruire un paradigma di spiegazione dell'operare dell'algoritmo e si prefigge di comprenderne il funzionamento, costruendone un modello. Gli studi più recenti hanno posto in evidenza che l'approccio di costruzione e di operatività dell'algoritmo non è quello modellistico, di creazione e spiegazione delle cause e degli effetti di un fenomeno, ma si struttura piuttosto come un metodo puramente statistico, tipico degli strumenti di intelligenza artificiale. Il *software* rimane dunque una *black-box*, un contenitore nel quale, come si è detto, i dati interagiscono senza che sia dato comprendere il percorso attraverso il quale si addiviene a un determinato risultato[36].

Il carattere di ontologica inaccessibilità del meccanismo di funzionamento[37] preclude ogni prova circa la scientificità dell'algoritmo, rendendolo insuscettibile di alcuna verifica. D'altro canto, va osservato che lo strumento in parola non individua affatto una successione di eventi con carattere di regolarità causale ma sintetizza il mero casuale avvicendarsi di fatti, strettamente dipendente dalle caratteristiche del luogo dal quale i dati sono stati tratti e dalle modalità con le quali è stato strutturato l'*input* del calcolo. Pare dunque che il risultato probatorio promanante dall'algoritmo non costituisca altro che un'evidenza statistica, che seppur utile in via generale e astratta, nulla può dire rispetto al singolo caso, necessitando di un'implementazione che tenga conto delle caratteristiche del caso oggetto di giudizio[38].

Sotto questo profilo, la dottrina d'oltreoceano ha evidenziato chiaramente che, in quegli ordinamenti che effettivamente si servono di tali strumenti, è imprescindibile un penetrante controllo sull'accuratezza dell'algoritmo prima di poterlo validamente porre alla base di qualsiasi decisione[39], affidandolo, se del caso, ad agenzie di controllo indipendenti[40].

Se da un lato la strutturale oscurità dell'algoritmo non permette verifiche accurate, dall'altro vi sono chiari elementi da cui inferire che tali strumenti presentano un elevatissimo tasso di errore[41]. L'algoritmo infatti è affetto da tutta una serie di *biases*, di fallacie cognitive, che si pongono sia al momento della formazione che al momento del concreto operare dello strumento.

Principiando dal momento formativo, è stato già evidenziato come alla base dell'algoritmo vi sia una scelta da parte dei programmatori circa i dati rilevanti da inserire quali *input*, dati che riflettono soltanto *few basic facts*[42], come il sesso, l'età, l'appartenenza ad un dato gruppo etnico, l'aver riportato precedenti condanne. Gran parte dei risultati dell'algoritmo non si fonda dunque su tutte le variabili che potrebbero avere rilievo nel concreto manifestarsi del reato, mancando informazioni sulla storia criminale, sulla gravità del fatto commesso, sulla stessa prognosi circa l'efficacia deterrente del processo e della condanna. Tale fallacia, definita *omitted variable bias*, mina l'affidabilità dell'algoritmo in maniera radicale.

Oltre a non riuscire a cogliere la completezza del fenomeno criminale, lasciando inalterata la cifra oscura[43], l'algoritmo riproduce, come si è già anticipato, disuguaglianze e disparità già presenti nel contesto sociale da cui i dati sono stati tratti. Un esempio concreto potrà forse chiarire tale asserzione. Si è avuto modo di accennare al fatto che uno degli algoritmi utilizzati in fase di *sentencing* e precisamente COMPAS, si basa sul fattore degli arresti. Se si assume

del metodo. Su quest'ultimo profilo si rinvia a Stella (2003), *passim*.

[35] Sul difetto di esaustività scientifica dell'algoritmo COMPAS, si veda Fronza, Caruso (2018), p. 197.

[36] Cfr. Henderson (2018), p. 532, che sottolinea come con gli algoritmi si effettui il percorso logico opposto a quello ordinariamente utilizzato nel processo: «*In traditional criminal investigations, police "move data to the question". They may want to know, say, who killed X or who stole from Y. So they gather evidence, moving data to the specific question at issue. Big data analysis does the opposite: store everything, and then "move the question to the data"*».

[37] In proposito v. Davis (2018), p. 6, che ritiene che il trascorrere del tempo e una maggiore trasparenza potrebbero non essere abbastanza per rendere accessibili e dunque utilizzabili gli algoritmi. Sulla necessità che gli algoritmi siano costruiti in modo da consentire un controllo sull'"eticità" dell'algoritmo stesso, v. Crisci (2018), p. 1790.

[38] Sull'argomento della prova statistica si vedano le fondamentali riflessioni di Stella (2003), p. 339 ss.

[39] Sottolinea questo profilo Carlson (2017), pp. 323 ss. In tema, cfr. anche Parodi, Sellaroli (2019), pp. 67-70.

[40] Cfr. Eaglin (2017), p. 122. Sotto questo aspetto, come evidenzia la dottrina d'oltreoceano, lasciare che gli algoritmi siano coperti dal segreto industriale non può fare altro che aumentare la competitività tra gli sviluppatori, a discapito della *fairness* dello strumento algoritmico medesimo.

[41] In argomento si vedano, nella dottrina italiana, le riflessioni di Crisci (2018), p. 1787, che evidenzia come siano proprio i *Big Data* ad avere un alto margine di errore e distorsione. In tal modo l'AI potrebbe apprendere informazioni non corrette in base alle quali poi prenderebbe decisioni non corrette e il tutto rischierebbe di generare un circolo vizioso di operazioni di trattamento dati autogenerate ed errate.

[42] Sottolinea questo aspetto Eaglin (2017), pp. 75 ss.

[43] Su tali profili si v. Eaglin (2017), p. 74.

quale criterio dirimente l'arresto (a cui non è detto segua poi la condanna) è evidente che, essendo la popolazione carceraria statunitense composta per la maggior parte da minoranze etniche, un soggetto di colore riporterà uno *score* di recidiva assai più elevato rispetto ad un altro soggetto non di colore. In questa prospettiva si è parlato di *racist algorithms*[44], algoritmi con pregiudizio razziale.

Un recente studio condotto dall'Agenzia di stampa no profit *Pro Publica*[45] ha posto in chiara evidenza proprio tale profilo. Sulla base di un'indagine condotta sullo stesso campione di persone utilizzato per costruire l'algoritmo COMPAS, *ProPublica* ha operato una valutazione dei dati scomposti per gruppi etnici e ha appurato che l'algoritmo è particolarmente fallace nell'etichettare i giovani di colore come futuri criminali, con un tasso di errore doppio rispetto ai soggetti bianchi. L'analisi normalizzata ha evidenziato infatti che gli accusati di colore risultavano avere il 77% di probabilità in più di essere indicati a rischio maggiore di commettere futuri crimini violenti.

L'indagine ha inoltre svelato l'elevatissimo tasso di errore degli algoritmi: dei potenziali recidivi individuati dal *software* solo il 20% aveva effettivamente commesso un nuovo crimine. Allargando l'analisi ai reati minori, poi, è stato evidenziato che il tasso di accuratezza degli algoritmi raggiungeva appena il 61%, l'equivalente del lancio di una moneta.

Un esempio varrà a chiarire meglio quanto sinora esposto. *Pro Publica* ha effettuato una comparazione tra due soggetti già sottoposti dapprima al giudizio di COMPAS, V.P., uomo appartenente alla maggioranza bianca, che aveva compiuto due rapine a mano armata e un tentativo di rapina a mano armata e B.B., donna appartenente alla minoranza di colore, che aveva commesso unicamente delle contravvenzioni in età giovanile. Quest'ultima era stata classificata ad alto rischio di recidiva (livello 8) a seguito del furto di una bicicletta per bambini, mentre il signor V.P. era stato classificato come soggetto a basso rischio (livello 3). Lo studio ha dimostrato che, in questa ipotesi, la signora B.B., pur essendo classificata ad alto rischio, non aveva posto in essere alcun ulteriore reato, differentemente dal signor V.P. che, seppur classificato a basso rischio, aveva immediatamente commesso una nuova rapina.

Alla luce di tutto quanto sino ad ora esposto pare proprio che l'algoritmo nasca affetto da una macropsia[46] di non poco momento, in quanto lo strumento ingigantisce determinati dati e restituisce punteggi falsati in eccesso rispetto a determinati soggetti, mettendo a serio rischio il principio di uguaglianza e di non discriminazione. Come trattare però "gli errori", che da algoritmici divengono giudiziari? È chiaro che essi hanno valenza diversa dal punto di vista informatico o da quello processuale. Uno dei profili di maggiore problematicità starà dunque nella reale capacità di contrastare le risultanze dell'algoritmo da parte delle difese.

5. Il diritto di difesa dall'algoritmo.

Se sul piano della scientificità del metodo le impressioni sono poco confortanti, non minori sembrano le criticità da segnalarsi sul piano del diritto di difesa.

Come si è avuto modo di anticipare, l'algoritmo predittivo è ordinariamente un algoritmo proprietario, coperto cioè da diritto d'autore; come tale, non è conoscibile né dalle Corti né dalle difese. Il problema è di rilievo cruciale in quanto, non essendo accessibile il meccanismo che si pone alla base dell'algoritmo stesso, ossia il modo in cui vengono a connettersi le informazioni già presenti nel calcolo e quelle relative al singolo caso, questo non è nemmeno controllabile dalla difesa. Da ciò consegue che nessun contraddittorio potrà esservi sull'ammissibilità dell'utilizzo dello strumento prima e sulle sue risultanze poi, con un evidente *vulnus* al principio del giusto processo.

L'inaccessibilità dell'algoritmo dunque non è soltanto ontologica ma si caratterizza anche

[44] Così Chander (2018), p. 1023.
[45] Lo studio condotto è reperibile al sito www.propublica.org/article/technical-response-to-northpointe. In argomento, cfr. Barbaro (2018), p. 194.
[46] Per macropsia si intende la visione ingigantita di oggetti in realtà distanti. In effetti pare che l'algoritmo ingigantisca il problema della recidiva con riferimento a determinati soggetti. Volendo utilizzare un'altra efficace espressione presa in prestito dal gergo oculistico, l'algoritmo produrrebbe una sorta di *visione a tunnel*. Per visione a tunnel si intende quell'insieme di tendenze sistematiche che impediscono di essere accurati nella percezione e nell'interpretazione degli eventi. Come negli ipovedenti, il campo visivo è così limitato da consentire di vedere unicamente ciò che si ha davanti agli occhi, escludendo la visione periferica, come all'interno di un tunnel, così la rappresentazione iniziale del problema può portare a non vedere altro che la prima risposta sorta nella mente, senza prendere in considerazione le altre variabili rilevanti per la soluzione del problema. Su questi argomenti v. Gulotta (2014).

come un'inaccessibilità-attributo, una voluta non ostensibilità[47]. Per la difesa sarà dunque impossibile effettuare qualsiasi controllo su struttura e funzionamento dell'algoritmo e ciò non può che ledere il diritto di difesa sia in astratto sia in concreto: il calcolo è padrone, poiché detta un criterio obiettivo contro il quale poco si può argomentare[48].

Per quegli ordinamenti che, nonostante tutti i profili critici appena evidenziati, consentono l'utilizzo di algoritmi predittivi in sede decisoria dovrebbe a monte assicurarsi una trasparenza sul meccanismo di funzionamento dello stesso, con una contestuale garanzia del più ampio contraddittorio sui risultati. In tale prospettiva, i risultati potrebbero essere oggetto di una presunzione solo relativa circa la futura commissione di un fatto di reato, passibile di prova contraria nel caso concreto.

6. L'algoritmo e il giudice "emotivo": il fenomeno dell'*anchoring* e il diritto alla valutazione individualizzata.

È indubbio che l'obiettività e la neutralità che caratterizzano il risultato prodotto dall'algoritmo conferiscono al *software* medesimo un grande fascino. Questo aspetto, tuttavia, pone un ulteriore e potente criticità rispetto all'utilizzo dello strumento in parola. La dottrina più accorta ha opportunamente evidenziato che l'algoritmo è in grado di esercitare pressioni interne ed esterne sul giudice che si appresta ad utilizzarlo; le pressioni esterne dipendono essenzialmente dal fatto che, per la loro oggettività, vi è una spinta dello stesso ordinamento verso l'adozione di strumenti che soddisfino i requisiti dell'efficienza e dell'affidabilità[49]. Al di là di tale pressione esterna, per converso, è necessario considerare che esistono *biases* psicologici che incoraggiano l'utilizzo di tali strumenti di *risk assessment*. Diversi studi evidenziano infatti che, quando gli algoritmi rimpiazzano il processo deliberativo umano, alla decisione finale viene conferita una sorta di "patina di inevitabilità" e, come immediata conseguenza, una "patina di correttezza"[50].

Il rischio che si crea però, è che i giudici si appoggino totalmente sul dato fornito dall'algoritmo, validandone le risultanze[51]. Tale fenomeno è noto, nella psicologia cognitiva, come *anchoring*, ossia quella tendenza comune per cui gli individui tendono ad affidarsi al mezzo di prova disponibile, senza avere riguardo alla debolezza esplicativa dello stesso, quando si trovino a dover prendere determinate decisioni[52]. Un giudice al quale viene fornita una valutazione del rischio che pronostica un alto tasso di recidiva potrebbe essere portato a irrogare una pena maggiore senza aver neanche la minima consapevolezza del ruolo avuto dall'"*anchoring*" nella decisione medesima[53].

L'algoritmo insomma è uno strumento dall'estrema persuasività e il suo manto di oggettività, che lo avvicina, nel suo aspetto esteriore, ad una prova scientifica, può condizionare fortemente il giudice al momento della decisione[54]. Il pericolo, tuttavia, è che il giudice possa rimanere irretito dal dato numerico e non prestare la dovuta attenzione a tutte le restanti risultanze probatorie, passando da un convincimento libero ad un convincimento intimo[55],

[47] Cfr. Davis (2018), p. 6, ove si evidenzia come la struttura dell'algoritmo sia talmente complessa e inaccessibile da non poter soddisfare la previsione di cui all'art. 22 del GDPR, che prevede il diritto di ciascun soggetto a conoscere il meccanismo attraverso il quale la procedura automatizzata arriva alle proprie conclusioni. L'A. afferma infatti: «*The GDPR includes a "right to explanation"- the right to demand an explanation for how an algorithm that affects a person reached its conclusions. What this will mean in practice is not clear. Government officials will have a difficult time defining what counts as a sufficient explanation. Does it have to be understandable? If so, to whom? The average person on the street? An expert? A few specialists in the relevant area? A hypothetical person with sufficient knowledge and intelligence to understand it, even if no one in fact possesses either? Does it just have to be technically correct and complete, even if abstruse-beyond human reckoning?*».

[48] Cfr. Simoncini (2018), p. 2 del dattiloscritto. Sul punto si rinvia alle riflessioni di Barbaro (2018), p. 194, che sottolinea come il principio di parità delle armi tra accusa e difesa potrebbe subire un *vulnus* a fronte dell'utilizzo degli algoritmi.

[49] *Harvard L. Rev.* (2017).

[50] In questo senso si rinvia a Chander (2017), p. 1034. In argomento, cfr., recentemente, Gialuz (2019), p. 22.

[51] *Harvard L. Rev.*, ove si ritiene «*challenging and unusual for individuals to defy algorithmic recommendations*».

[52] In argomento deve rinviarsi alle fondamentali riflessioni di Tversky, Kahneman (1982), p. 14. Di particolare interesse poi è il contributo di Chapman L., Chapman J. (1982), p. 239 ss., in particolare sul fenomeno dell'*illusory correlation*.

[53] *Harvard L. Rev.*, p. 1536. Sul ruolo delle illusioni cognitive nel ragionamento giudiziario cfr. Cevolani, Crupi (2018), p. 21.

[54] Su questi aspetti si rinvia, per tutti, a Dominioni (2005), ove evidenzia come si determini nei giudici un errato convincimento come se gli elementi forniti dalla prova scientifica siano tali da prestarsi a una valutazione oggettiva e che il giudice debba in questi casi abdicare alla sua funziona valutativa.

[55] Per convincimento intimo si intende quella persuasione interiore rigorosamente soggettiva, non razionalizzabile e non controllabile, v. da ultimo Taruffo (2014), p. 1242. Sull'impatto potenzialmente negativo sull'imparzialità del magistrato da parte dell'algoritmo, v. Barbaro

concentrandosi cioè più sulla tipologia d'autore che sul fatto oggetto del processo[56]. Tutto ciò implica altresì il possibile verificarsi di gravi inversioni argomentative, tali per cui il giudice possa anche considerare l'imputato colpevole per il fatto oggetto di giudizio solo in base alla futura probabilità di commettere reato, valutata secondo le risultanze dello strumento di intelligenza artificiale.

Pare in definitiva che l'algoritmo non possa che rafforzare i c.d. *stereotipi impliciti*, fisiologicamente presenti nella persona che deve effettuare un giudizio, aumentando il rischio di condannare a pene elevate soggetti appartenenti a determinate categorie personologiche[57]. A fronte di ciò, a poco varrà sostenere, come accaduto nella vicenda di Eric Loomis, che il giudice conserva il governo sul dato numerico, poiché l'algoritmo "elimina il lavoro", si impone per la sua forza pratica, consente al giudice di non spiegare nulla[58]. Il *software* predittivo è infatti un comodo riparo per il giudice che, nascondendosi dietro lo *score*, potrebbe omettere di considerare tutte le peculiarità del caso e, come immediata conseguenza, omettere di motivare adeguatamente in ordine alla commisurazione della pena[59].

Tutto quanto sinora esposto, poi, non deve far dimenticare il nodo cruciale dell'utilizzo di tali strumenti, ossia la spersonalizzazione dell'imputato in una parte del procedimento che conduce alla decisione sulla commisurazione della pena. L'algoritmo formula infatti una prognosi, l'effetto della quale è estendere all'imputato i risultati di una generalizzazione, portando al contempo il giudice ad una valutazione sempre meno individualizzata[60]. In questo modo si crea il pericolo di standardizzare il singolo caso, facendolo confluire nella mera statistica e le peculiarità del singolo accadimento rischierebbero di sfumare nella nuvola delle probabilità.

In ultimo, come accorta dottrina non ha mancato di sottolineare, l'ostacolo reale dell'algoritmo predittivo del rischio di recidiva sta nell'impossibilità per lo stesso di elaborare il concetto di revisione critica[61], di ripensamento del rischio reato[62]. Ciò che l'algoritmo non riesce a considerare, perlomeno allo stato, è l'effetto che la vicenda processuale e la sentenza di condanna possono avere sulla reale prognosi di recidiva[63].

6.1. *L'insormontabile divieto di perizia psicologica quale argine al potere dell'algoritmo.*

Ove tutto ciò non fosse sufficiente a escludere un possibile utilizzo degli algoritmi predittivi, pare comunque che nel nostro ordinamento esista già un presidio che possa impedire la loro diffusione: il divieto di perizia psicologica *ex* art. 220 c.p.p. È noto che il codice di procedura penale vieta al giudice di servirsi di perizie per stabilire l'abitualità o la professionalità nel reato, la tendenza a delinquere, il carattere e la personalità dell'imputato e in genere le qualità psichiche indipendenti da cause patologiche, soprattutto al fine di evitare che il giudicante possa rimanere condizionato dalle valutazioni sul carattere dell'imputato, tralasciando di apprezzare adeguatamente il fatto oggetto di giudizio[64].

(2018), p. 194.

[56] *Harvard L. Rev.*, p. 1536; Carlson (2017), p. 303 ss.; Eaglin (2017), pp. 59 ss. che parla di "indirizzamento della discrezione del giudice al momento della sentenza".

[57] In tema si veda *supra*, par. 3, nota 23.

[58] Simoncini, dattiloscritto, ove parla del risultato dell'algoritmo nei termini di una *default option.*

[59] L'algoritmo potrebbe dunque rafforzare la decisione del giudice che, secondo gli psicologi cognitivi, si connota come un fatto per lo più intuitivo e non razionale. Le emozioni suscitate nel giudicante dalla vicenda umana lo guidano infatti in anticipo, finendo per condizionarlo inconsciamente. Su tutti tali aspetti si rinvia all'interessante indagine di Forza, Menegon, Rumiati (2017), p. 144 ss., ove si evidenzia, più in generale, come la libertà valutativa alla base del libero convincimento si caratterizzi come una discrezionalità incontrollata, sinonimo di intuizione personale, di sentimento, di emozione se non addirittura di credo ideologico, di valori e di soggettive visioni del mondo. Gli A. sottolineano infatti come l'istinto, l'intuizione, le emozioni e la soggettività siano fenomeni psicologici del tutto ignorati dalla dottrina processual-penalistica che dovrebbero tuttavia essere oggetto di particolare attenzione onde prevenire ed evitare possibili errori giudiziari. Sul tema v. anche Cevolani, Crupi (2018), *passim*; Gaboriau (2018), p. 212.

[60] In argomento v. Forza, Menegon, Rumiati (2017), p. 89.

[61] Su questi temi cfr. Eusebi (2013), p. 1307 ss.

[62] Si condivide dunque quanto ritiene Barbaro (2018), p. 192, che evidenzia come il più grande limite dell'intelligenza artificiale consista nell'incapacità di adattare il suo funzionamento al di fuori del proprio modello.

[63] Cfr., Eaglin (2017), p. 100. La Corte costituzionale, peraltro, ha in diverse occasioni sottolineato la necessità che il giudice effettui una prognosi di recidiva più individualizzata possibile, nell'opera di progressiva demolizione di tutte quelle ipotesi normative che prevedevano un'applicazione obbligatoria dell'aumento di pena *ex* art. 99 c.p. Sul punto si rinvia, tra le altre, a Corte cost., 23 luglio 2015, n. 185, in www.cortecostituzionale.it; Corte cost., 17 luglio 2015, n. 270, in www.cortecostituzionale.it.

[64] Si rinvia, in argomento, all'interessante contributo di Moscarini (2006), p. 169. Sul punto cfr. anche Moffetti (2013), p. 357 ss.

Ebbene, se si analizzano le domande del questionario che si sottopone al reo, momento fondamentale in cui raccogliere i dati sul caso concreto da inserire poi nel meccanismo di COMPAS, si può facilmente notare come all'imputato vengano richieste informazioni sulla propria personalità e il proprio carattere[65]; vi sono quesiti ad esempio sul tempo libero, sulle inclinazioni personali, sulle capacità di reazione agli stimoli esterni, sul carattere, sulla fiducia nella giustizia, sull'importanza dei legami familiari. Tale questionario, somministrato peraltro al momento meno garantito dell'intera vicenda processuale, quello dell'arresto, si compone di tutta una serie di domande volte a ottenere informazioni che il giudice non potrebbe conoscere.

Una sezione del questionario, ad esempio, è dedicata alle domande sull'isolamento sociale del reo, si richiede di esprimere il livello di accordo con alcune statuizioni come ad esempio: "mi sento solo? Mi sento infelice a volte? Quanto spesso ci si sente annoiati?".

Una diversa sezione del questionario è dedicata poi all'attitudine criminale, si chiede infatti al reo di indicare il livello di adesione rispetto a certe asserzioni come: "quando le persone compiono reati minori o usano droghe non fanno danno a nessuno"; "se qualcuno insulta i miei amici, la mia famiglia o il mio gruppo avrà problemi"; "la legge non aiuta le persone medie"; "alcune persone non meritano alcun rispetto e dovrebbero essere trattate come animali".

Pare si tratti insomma di vere e proprie informazioni sulla personalità che vengono sottratte a qualsiasi controllo, entrando a far parte della base di calcolo del *software*, con il rischio indurre il giudice a soffermarsi più sulla persona che sul fatto nella sua oggettività, aggirando così il divieto di cui all'art. 220 c.p.p.

7. I possibili spazi applicativi dell'algoritmo tra esigenze di sicurezza e imprescindibili garanzie.

Nel contesto descritto pare quindi doversi concludere che algoritmi e processo penale si pongano tra loro in termini di reciproca esclusione. A venire meno sarebbe il profilo caratteristico della vicenda reato, ossia la dimensione di umanità, con la quale è imprescindibile confrontarsi[66]. «Tutto ciò che fa l'algoritmo lascia fuori di sé una domanda sulla natura più intima dell'uomo. Si potrà definire una nuova procedura meccanica più perfezionata che ci aiuti a rispondere a tale questione ma ci sarà sempre una domanda inevasa sul carattere precipuo della nostra identità e del nostro discernimento»[67].

Se all'interno della dialettica processual-penalistica l'algoritmo non può trovare spazio alcuno per le ragioni appena evidenziate, lo stesso non va demonizzato, potendo essere piuttosto inteso come un mezzo utile a razionalizzare le risorse verso una maggiore efficienza sistemica. In tale prospettiva, possibili spazi applicativi dell'algoritmo potrebbero aversi nella sfida di prevenzione del rischio reato. In effetti gli strumenti algoritmici si stanno imponendo anche in Italia come sistema per indirizzare gli sforzi delle forze di Polizia verso una più proficua strategia di prevenzione del crimine[68].

[65] L'intero questionario è reperibile all'indirizzo web https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE.html.

[66] Sul profilo della giustizia digitale che dematerializza il conflitto e rende non necessario l'incontro tra le parti si veda Garapon, Lassegue (2018). Tutto ciò in contrasto con le più moderne tendenze della giustizia riparativa, che mirano, all'opposto, a promuovere l'incontro tra reo e vittima ai fini dell'elaborazione del conflitto. Sullo specifico profilo della *restorative justice* come momento di confronto tra parti contrapposte si rinvia a Mannozzi (2017).

[67] Zellini (2018), p. 19 ss. Sull'argomento dell'insostituibilità dell'uomo con lo strumento algoritmico Crisci (2018), p. 1795 ss.

[68] In argomento cfr. Koss (2015), pp. 301 ss. ove l'A., riferendosi all'esperienza statunitense, paventa una possibile violazione del Quarto emendamento della Costituzione americana, che sancisce il diritto alla *privacy*. Su questi profili si vedano anche le riflessioni di Simmons (2016), pp. 947 ss. In tema, cfr. altresì Bonfanti (2018), p. 2. L'utilizzo degli algoritmi si sta imponendo anche in Italia nell'ambito della prevenzione di polizia. Le Forze dell'Ordine stanno infatti sperimentando un algoritmo denominato X-LAW attraverso il quale si vanno a monitorare alcune porzioni territoriali utilizzando la tecnica del *crime mapping*. Tale algoritmo, sviluppato dall'ispettore capo Lombardo della Questura di Napoli, e di cui si può leggere in un interessante studio condotto dall'Università di Napoli Federico II del 2017, rielabora dati storici e urbani pre-inseriti nel sistema sulla base delle denunce, dei luoghi e delle ore ove il crimine è stato perpetrato, delle informazioni sui media e delle informazioni demografiche e sociali. Sono poi inseriti il numero dei cittadini, gli eventi pubblici, la presenza di insediamenti economici, la popolazione dimorante nei diversi quartieri. Tutti questi dati costituiscono la base dell'algoritmo, che si fonda sulla considerazione che chi commette reati predatori è al 90% un criminale seriale, che agisce nella stessa zona con le stesse modalità. In tal maniera l'algoritmo riesce a fornire un *alert* che indirizza la polizia verso un determinato luogo ove è più probabile che il crimine medesimo avvenga. In effetti l'utilizzo sperimentale di tale algoritmo ha da ultimo condotto, nell'area della città di Venezia, a sventare un crimine nell'84 % dei casi segnalati tramite *alert*. L'algoritmo dunque è lo strumento per rivoluzionare l'approccio della polizia che dal rincorrere il criminale passa ad anticiparlo,

Ma l'algoritmo potrebbe altresì essere valorizzato su di un piano differente da quello appena esaminato. Il suo ruolo potrebbe infatti essere quello di strumento funzionale alla predisposizione di una più adeguata e meno superficiale politica di prevenzione speciale.

A tal fine, gli algoritmi potrebbero essere sviluppati in modo da rendere il dato finale maggiormente aderente al singolo caso in questione. Se il problema è che nella *black-box* algoritmica i dati personali perdono la loro specificità, allora, con il progredire tecnologico, si dovrebbe implementare il *software*, fare in modo che lo stesso assicuri una maggiore ponderazione delle informazioni sul singolo caso nel risultato del calcolo.

In questa prospettiva, con una più intensa collaborazione tra programmatori dell'algoritmo e esperti di diritto[69], si potrebbe pensare di costruire un questionario meglio calibrato, privo di domande eccessivamente invasive circa la personalità del soggetto, e fare sì che i dati emergenti dal questionario stesso rivestano un peso maggiore rispetto ai dati già presenti nella base dell'algoritmo. Così operando, l'algoritmo potrebbe esprimere un risultato che abbia aderenza maggiore alle peculiarità del caso singolo.

Una volta migliorato l'algoritmo, si potrebbe allora tenere conto dei dati elaborati come un elemento per formulare più accurate valutazioni in ordine alla prognosi di recidivanza in sede di concessione della sospensione condizionale, come anche al momento della decisione sull'ammissione alle misure alternative alla detenzione; l'algoritmo insomma potrebbe essere in grado di fornire le informazioni necessarie a commisurare con maggiore accuratezza il trattamento sanzionatorio specificamente dedicato alle peculiarità del singolo condannato, facendo salve le imprescindibili garanzie dello stesso, atteso che l'azione del *software* potrebbe dispiegarsi solo in un momento successivo alla valutazione della sussistenza della responsabilità. In tale prospettiva, si potrebbe tenere conto delle risultanze provenienti dall'algoritmo nella determinazione del *contenuto* della condanna da intendersi come un *progetto* e non più come mera retribuzione[70], dando così linfa nuova alla funzione di risocializzazione della pena.

Infine, la complessità delle questioni qui descritte raggiunge un livello ancora più profondo se si pone mente alle più recenti acquisizioni provenienti dal sapere neuroscientifico[71]. L'idea di predeterminazione alla commissione di un fatto di reato veicolata dall'algoritmo, associata alla prospettiva neuroscientifica, che nelle sue versioni forti ripropone l'idea di una fisiologica predisposizione al reato[72], rievoca il concetto di forza del destino, di ineluttabilità per alcuni soggetti di una ricaduta nel fatto criminoso. Ciò che, sia gli algoritmi che le neuroscienze mettono in questione, insomma, è la reale portata del concetto di autodeterminazione della persona.

Come la dottrina più attenta ha puntualmente evidenziato, il concetto di libertà del volere è diversamente declinato a seconda dell'ambito e degli obiettivi della disciplina di riferimento (psicologia, diritto, etc.): il diritto penale pone al centro del giudizio di responsabilità proprio la libertà del volere. Nella prospettiva penalistica, negare tale libertà significherebbe disconoscere l'autore del reato come persona e come membro della società, posto che la dignità dell'individuo sta proprio nella possibilità di muovergli un rimprovero, che presuppone una piena colpevolezza. Secondo tale dottrina il sapere neuroscientifico, dunque, dovrà essere valorizzato non in una prospettiva di abbandono del diritto penale classicamente inteso ma in un senso costruttivo, come strumento che, fornendo una base conoscitiva più ampia dello stato del condannato, possa arricchire le modalità di risposta al reato nel rispetto dei principi fondamentali di proporzionalità e di dignità della persona[73].

Seguendo questa prospettiva anche rispetto alle questioni poste dagli algoritmi predittivi, i progressi tecnologici non potranno più essere visti come "segnali di allarme" dell'insufficienza delle categorie del diritto penale classico, potendo invece fornire un importante contributo per rendere più efficiente l'intero sistema, che potrebbe trovare rinnovato vigore applicativo

controllando le c.d. zone di caccia Anche in questo caso non si può confidare in assoluto su tale strumento in quanto lo stesso ha un tasso di errore tipico di ogni calcolo probabilistico. Inoltre non può nemmeno affidarsi del tutto alla Forza Pubblica il compito di prevenzione: le zone maggiormente a rischio infatti sono tali per problemi socio economici endemici e certamente non risolvibili con il solo intervento delle Forze armate. L'algoritmo non è tuttavia in grado da solo di risolvere i problemi, dovendo piuttosto essere inteso come uno strumento che per funzionare dovrà essere integrato nel sistema generale di prevenzione di disagi sociali e programmazione di azioni finalizzate a migliorare la qualità della vita, attraverso una riqualificazione e una gestione degli spazi pubblici.

[69] Cfr., sul punto, le riflessioni di Gialuz (2019), p. 21.

[70] Per una prospettiva di questo tipo rispetto al problema della risposta al reato v. Eusebi (2013), p. 527.

[71] In argomento si rinvia a Bertolino (2015), p. 85 ss.; Grandi (2014), p. 1249 ss.

[72] Sul tema, cfr. Bertolino (2015), p. 86; Ead., (2008), p. 325 ss.

[73] Così Bertolino (2015), p. 96.

proprio valorizzando le nuove acquisizioni della tecnica.

Bibliografia

Barbaro, Clementina (2018), *"Uso dell'intelligenza artificiale nei sistemi giudiziari: verso la definizione di principi etici condivisi a livello europeo? I lavori in corso alla Commissione europea per l'efficacia della giustizia (Cepej) del Consiglio d'Europa"*, *Questione Giustizia*, 4, pp. 189-195.

Bertolino, Marta (2015), "*Il vizio di mente tra prospettive neuroscientifiche e giudizi di responsabilità penale*", *Rassegna italiana di criminologia,* 2, pp. 84-97.

Bertolino, Marta (2008), "*Il "breve" cammino del vizio di mente. Un ritorno al paradigma organicistico?*", *Criminalia*, pp. 325-346.

Bonfanti, Angelica (2018), "Big Data *e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy*", *Media Laws – Rivista di diritto dei media*, 3, in corso di pubblicazione.

Brennan Dieterich (2018), *"Correctional offenders management profiles for alternatives sanctions"*, in Singh J.P. *et al*, *Handbook of Recidivism Risk/Needs Assessment tools*, John Wiley and Sons, New York.

Carlson, Alyssa M. (2017), "*The Need for Trasparency in the Age of Predictive Sentencing Algorithms*", *103 Iowa Law Review*, pp. 303- 329.

Castelli Claudio e Piana Daniela (2018), *"Giustizia predittiva. La qualità della giustizia in due tempi"*, *Questione Giustizia*, 4, pp. 153-165.

Cevolani Gustavo e Crupi Vincenzo (2018), *"Come ragionano i giudici: razionalità, euristiche e illusioni cognitive*, *DisCrimen*, 22 ottobre 2018.

Chander, Anupam (2017), "*The Racist algorithm*", 115 *Michigan Law Review*, pp. 1023-1045.

Chapman Loren J. e Chapman Jean (1982), "*Test results are what you think they are*", in Kahneman D. *et al.*, *Judgement under uncertainty: Heuristics and biases*, Cambridge, Cambridge University Press, pp. 239-249.

Costanzi, Claudio (2018), *"La matematica del processo: oltre le colonne d'Ercole della giustizia penale"*, *Questione Giustizia*, 4, pp. 166-188.

Crisci, Stefano (2018), *"Intelligenza artificiale ed etica dell'algoritmo*", *Foro Amministrativo*, 10, pp. 1787-

Davis, Joshua P. (2018), *"Law without mind. AI, Ethics and Jurisprudence*, 5 *University of San Francisco Law research Paper.*

De Mauro, Tullio (2000), *Dizionario della lingua italiana*.

Dick, Philip K. (2002), "*The Minority Report*", Pantheon Books, New York.

Dominioni, Oreste (2005), *"La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Milano, Giuffrè.

Eaglin, Jessica M., (2017), "*Constructing recidivism risk*", *67 Emory Law Journal*, pp. 59-122.

Eusebi, Luciano (2013), *"La riforma ineludibile del sistema sanzionatorio penale"*, *Rivista italiana di diritto e procedura penale*, pp. 1307-1328.

Eusebi, Luciano (2013), "*La risposta al reato e il ruolo della vittima*", *Diritto penale e processo*, 5, pp. 527-531.

Forti Gabrio (2000), *"L'immane concretezza. Metamorfosi del crimine e controllo penale"*, Milano, Raffaello Cortina Editore.

Forza Antonio, Menegon Giulia e Rumiati Rino (2017), *"Il giudice emotivo. La decisione tra ragione ed emozione"*, Bologna, Il Mulino.

Fronza, Emanuela e Caruso Corrado (2018), *"Ti faresti giudicare da un algoritmo? Intervista a Antoine Garapon"*, *Questione Giustizia*, 4, pp. 196-199.

Gaboriau, Simone (2018), *"Libertà e umanità del giudice: due valori fondamentali della giustizia. La giustizia digitale può garantire nel tempo la fedeltà a questi valori?"*, in *Questione Giustizia*, 4, pp. 200-211.

Garapon, Antoine e Lassègue, Jean (2018), "*Justice digital. Révolution grafique et rupture antropologique"*, PUF, Paris.

Gialuz Mitja (2019), "*Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa"*, *Diritto penale contemporaneo*, 29 maggio 2019.

Grandi, Ciro (2014), *"Sui rapporti tra neuroscienze e diritto penale"*, *Rivista italiana di diritto e procedura penale*, 3, pp. 1249-1290.

Gulotta, Guglielmo (2014), "*Psicologia dell'errore nell'investigazione e nel giudizio"* in De Cataldo Neuburger L. (a cura di), *"«L'operazione decisoria» da emanazione divina alla prova scientifica. Passando per Rabelais*, Padova, Cedam.

Isaac, William S., *"Hope, Hype and Fear: The Promise and Potential Pitfalls of Artificial Intelligence in Criminal Justice"*, 15 *Ohio State Journal of Criminal Law*, pp. 543-558.

Joyce, Peter (2018), "*Criminology and Criminal Justice. A study guide*", Routledge, London and New York.

Koss, Kelly K. (2015), "*Leveraging Predictive Policing Algorithms to Restore Fourth Amendament Protections in High crime Areas in a Post Wardlow World"*, *90 Chicago-Kent Law Review*, pp. 301-334.

Moffetti, Rita Caterina (2013), "*La perizia psicologica tra processo ordinario e processo minorile"*, *Archivio della nuova procedura penale*, 4, pp. 357-361.

Moscarini, Paolo (2006), "*La perizia psicologica e il "giusto processo"*, *Diritto penale e processo*, 8, pp. 929-932.

Parodi, Cesare e Sellaroli Valentina (2019), *"Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco"*, in *Diritto penale contemporaneo*, 6, pp. 47-71.

Simmons, Ric, (2018), *"Big Data and Procedural Justice: Legitimizing Algorithms in the Criminal Justice System"*, 15 *Ohio State Journal of Criminal Law*, pp. 573-581.

Simmons, Ric, (2016), "*Quantifying criminal procedure: how to unlock the potential of Big Data in our criminal justice system*, *Michigan State Law Review*, pp. 947-1017.

Singh *et al* (2018), *Handbook of Recidivism Risk/Needs Assessment tools*, John Wiley and Sons, New York.

Stella, Federico (2003), *"Giustizia e modernità. La protezione dell'innocente e la tutela delle vittime"*, Giuffrè, Milano.

Taruffo, Michele (2016), "*La decisione giudiziaria e la sua giustificazione: un problema per le neuroscienze*?", *Rivista trimestrale di diritto e procedura civile*, pp. 1239-1251.

Tversky Amos e Kahneman Daniel (1982), *Judgement under uncertainty: Heuristics and biases*, in Kahneman D. et al., *Judgement under uncertainty: Heuristics and biases*, Cambridge, Cambridge University Press.

Viola, Luigi (2018), "*L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*", *Foro Amministrativo*, 9, pp. 1598-1640.

Zellini, Paolo (2018), "*La dittatura del calcolo*", Milano, Adelphi.

Le nuove indagini tecnologiche e la tutela dei diritti fondamentali. L'esperienza del captatore informatico

Las nuevas tecnologías de investigación y la tutela de los derechos fundamentales. La experiencia del software espía

New IT-based Investigations and Protection of Fundamental Rights. The Case of Spy-software

Gaia Caneschi
Dottoressa di ricerca in giustizia penale e internazionale presso l'Università Bocconi di Milano
gaia.caneschi@unibocconi.it

Diritti fondamentali, Intercettazioni
Derechos fundamentales, Interceptación de comunicaciones
Fundamental rights, Intrusive surveillance

Abstracts

Nonostante l'ampia diffusione nella prassi, è solo negli ultimi tempi, anche grazie all'acceso dibattito suscitato da alcune pronunce della Corte di cassazione, che l'attenzione degli interpreti si è concentrata sul c.d. captatore informatico, un vero e proprio virus dotato di capacità intrusive formidabili, che viene inoculato da remoto in un dispositivo informatico e che consente lo svolgimento di numerose attività di indagine con modalità tecnologicamente avanzate.
La portata delle potenzialità investigative dello strumento sembra essere sfuggita al legislatore che, solo di recente, ne ha regolamentato l'impiego investigativo esclusivamente come strumento di intercettazione di comunicazioni tra presenti.
Adagiandosi sull'ormai invalsa tecnica legislativa che considera le decisioni della Corte di cassazione alla stregua di "proposte" di legge, l'intervento del legislatore non può che essere ritenuto, soprattutto per i suoi "non detti" (non sono infatti disciplinate alcune delle più invasive funzioni del captatore informatico), complessivamente inadeguato rispetto alla tutela dei diritti fondamentali in gioco.

A pesar de la práctica generalizada, es solo en los últimos tiempos, también gracias al acalorado debate provocado por algunos juicios del Tribunal Supremo italiano, que la atención de los intérpretes se ha centrado en el c.d. software espía, un virus con capacidades intrusivas formidables, que se inocula remotamente en un dispositivo informático y que permite realizar numerosas actividades de investigación con métodos tecnológicamente avanzados.El alcance del potencial investigativo del instrumento no parece haber sido entendido por el legislador que, recientemente, ha regulado su uso investigativo exclusivamente como una herramienta para interceptar las comunicaciones entre los presentes. De hecho, la intervención del legislador debe considerarse inadecuada con respecto a la protección de los derechos fundamentales en juego, especialmente porque algunas de las funciones más invasivas no están reguladas.

Despite a wide diffusion, only in recent times the attention of the interpreters has been drawn on the spyware, a malware with high intrusive skills, which is installed in a target device and allows to perform a lot of investigation activities. The legislator does not seem to have fully considered the magnitude of these potential uses, having recently disciplined the spyware only as a tool for audio surveillance. Due to the uncovered areas (which relate to some of the most intrusive skills of the spyware), the discipline introduced by the legislator does not appear to be adequate, considering the need of protection of the fundamental rights at stake.

Sommario

1. Un *virus* informatico al servizio delle indagini.

È ormai acquisita al patrimonio delle conoscenze comuni l'esistenza e l'ampia diffusione nella prassi di *virus* occulti che consentono lo svolgimento di attività investigative dall'elevato potenziale intrusivo che fino a pochi anni fa apparivano impensabili.

I c.d. "captatori informatici", anche chiamati con un'espressione molto evocativa "*trojan horse*", sono *software* che possono essere introdotti fisicamente in un sistema informatico, oppure essere inviati da remoto, per esempio come allegato *mail* o come aggiornamento di applicazioni, che acquisiscono di fatto il controllo dell'apparecchio in cui vengono inoculati.

L'elenco delle attività che possono essere svolte mediante il captatore è impressionante: leggere quello che è archiviato nel dispositivo, dal contenuto dei documenti di testo alla rubrica dei contatti, fino alle comunicazioni scambiate via *Whatsapp*, *Telegram*, *Messenger*; gestire da remoto i *software* che vengono installati; scaricare immagini e filmati e controllare quelli presenti nelle gallerie; memorizzare i pulsanti premuti sulla tastiera e fare lo *screenshot* di quello che compare sullo schermo; collegarsi ad *internet*; inserire dati o alterare quelli esistenti; rintracciare gli spostamenti se l'apparecchio infettato è dotato di sistema *gps*; accendere il microfono o la telecamera consentendo di svolgere un'intercettazione ambientale o una videoripresa; tutte funzioni che possono essere calibrate sulla base delle esigenze del caso specifico adottando opportuni accorgimenti tecnici ([1]).

La dotazione di strumentazioni del genere per lo svolgimento delle indagini è resa indispensabile dal fatto che le più evolute (ed insidiose) forme di manifestazione del crimine si avvalgono della tecnologia informatica per la commissione dei reati: così, lasciare gli inquirenti sforniti di mezzi di ricerca della prova adeguati rispetto ai più avanzati fenomeni delinquenziali equivarrebbe ad accettare l'idea di un processo penale che, per ragioni di fisiologica obsolescenza di alcuni dei propri istituti, non è in grado di assicurare un compiuto accertamento dei fatti.

Se da un lato, dunque, appare indispensabile riconoscere l'importanza dell'accesso a tali nuovi strumenti tecnologici per perseguire un'efficace azione di contrasto del crimine, dall'altro lato, estremamente delicato è individuare i confini del loro impiego ai fini investigativi, alla ricerca di un equilibrio con la confliggente esigenza di tutela dei diritti fondamentali degli individui coinvolti nella vicenda processuale.

Libertà personale, libertà domiciliare, libertà di comunicazione e di corrispondenza, ma anche dignità e riservatezza, infatti, sembrano meritare una moderna ridefinizione alla luce delle nuove forme di potenziale aggressione che possono derivare dall'impiego dei *virus* di cui si parla.

2. Indagini tecnologiche e tutela dei diritti fondamentali.

In alcuni ordinamenti, le enormi potenzialità intrusive che derivano dall'utilizzo ai fini investigativi delle nuove tecnologie non sono sfuggite e hanno progressivamente portato al riconoscimento di diritti fondamentali prima inediti: il caso esemplificativo è quello della Germania, la cui Corte costituzionale, già nel 2008, ha affermato l'esistenza del diritto all'uso confidenziale dei sistemi informatici, o meglio del «diritto alla garanzia dell'integrità e della riservatezza dei sistemi informatici», enucleato dall'obbligo che lo Stato ha di tutelare la dignità dei propri cittadini di fronte a qualsiasi aggressione, inclusa quella che proviene dall'autorità

[1] Sottolineano le potenzialità intrusive del captatore informatico Camon (2017a), p. 91; Felicioni (2016), p. 123; Filippi (2016), p. 351; nonché, diffusamente sul piano tecnico, Brighi (2018) p. 211.

pubblica ([2]).

Come si sa, l'individuazione di un nuovo diritto inviolabile non impedisce all'ordinamento di operare un giudizio di bilanciamento che comporti la sua limitazione in rapporto ad altre esigenze che sono ritenute indispensabili per la tutela dei consociati, come quella che riguarda la prevenzione e la repressione dei reati ([3]). Tuttavia, la compressione di un diritto che appartiene al rango di quelli che l'ordinamento considera fondamentali richiede che sia la legge a definire i casi e i modi della limitazione, nonché che vi sia una motivata autorizzazione giudiziale nel rispetto del principio di proporzionalità ([4]).

Viene allora da domandarsi quale potrebbe essere la strada per il riconoscimento di un'inedita libertà fondamentale che tenga conto dei possibili sviluppi della personalità umana legati all'impiego della tecnologia informatica ([5]).

Se ci si limitasse a considerare quale connotato decisivo della nuova libertà la sola dimensione per così dire "statica" della riservatezza dei dati informatici, si potrebbe ritenere che essa sia già tacitamente inclusa nell'art. 2 Cost. ([6]). Ma la norma in questione predispone una forma di tutela che, oltre a proteggere il solo aspetto relativo alla *privacy* e dunque a non rappresentare pienamente la portata rivoluzionaria del fenomeno della "*smartphone addiction*", non risolve il problema della regolamentazione dei rapporti tra Stato e cittadino, sotto il profilo delle limitazioni che il primo può imporre al secondo ([7]).

Un modello forte di tutela, grazie alla previsione di riserve rinforzate, potrebbe derivare dalla enucleazione – ad opera della Corte costituzionale – di nuove estensioni degli artt. 13, 14 e 15 Cost., la cui latitudine potrebbe essere tale da offrire tutela anche ad espressioni evolute delle libertà fondamentali in essi enunciate.

Per questa via, si può facilmente osservare che, in effetti, la stessa idea di libertà personale potrebbe essere compromessa da un utilizzo perdurante del captatore informatico su un qualsiasi apparecchio informatico di uso quotidiano: in ipotesi del genere, l'attività d'indagine espletata tramite il *virus* si tramuterebbe in una forma di sorveglianza occulta e continuativa del *device* e di chi lo usa ([8]).

Il concetto di libertà personale non verrebbe affatto stravolto: nel corso del tempo, infatti, esso ha assunto una dimensione molto ampia, non più concepito come garanzia esclusiva dell'*habeas corpus*, bensì esteso fino a comprendere la pretesa al libero sviluppo della persona umana, dunque inteso anche in un'accezione comprensiva della libertà morale che, indubitabilmente, potrebbe entrare in contrasto con l'impiego indiscriminato del *virus* informatico ([9]).

Tra l'altro, la Corte costituzionale aveva già riconosciuto che «i contenitori portatili che (…) trovano diretta copertura nelle garanzie dell'art. 13 Cost. sono soltanto quelli che attengono alla sfera della libertà personale, e perciò quelli che abitualmente sono portati sulla persona

[2] Si allude alla sentenza 27 febbraio 2008 del *Bundesverfassungsgericht*, 1 BvR 370/07 – 595/07, analizzata da Flor (2009) p. 695. Un'altra decisione della Corte costituzionale tedesca sul tema è *Bundesverfassungsgericht*, 1 BvR 966/09, 1 BvR 1140/09, 20 aprile 2016, i cui contenuti sono commentati da Venegoni e Giordano (2016) e da Nicolicchia (2017). Quello dell'ordinamento tedesco non è l'unico caso di presa di coscienza dell'impatto dell'evoluzione tecnologica nel processo penale: leggi sul *trojan virus* sono state introdotte in Spagna, in Francia e nel Regno Unito e proposte di riforma sono discusse anche in altri Paesi europei (Paesi Bassi e Portogallo). Sulle iniziative di riforma nei Paesi Bassi e in Spagna in particolare si rinvia a Iovene (2014), p. 331. V. inoltre il progetto di studio della Commissione Libertà civili, giustizia e affari interni del Parlamento europeo: «*Legal Framework for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*» (2017), un'analisi comparata avente ad oggetto sei Stati membri dell'Unione Europea (Francia, Germania, Italia, Paesi Bassi, Polonia e Regno Unito) ed altri Stati non appartenenti Unione Europea (Australia, Israele e Stati Uniti).

[3] Una tutela "progressiva" dei diritti è teorizzata da Orlandi (2014) p. 1133, nel senso di tenere conto, da un lato, di un loro opportuno adeguamento all'evoluzione tecnologica e, dall'altro lato, della loro costante condizione di tensione con l'esigenza di repressione dei reati. Cfr. Felicioni (2015), p. 40, la quale considera che le libertà fondamentali sono più esposte a «limitazioni più o meno estese in nome dell'efficienza del processo».

[4] Tale principio, anche se non formalizzato nel nostro ordinamento, assume un ruolo fondamentale nel giudizio di bilanciamento dei diritti, cfr. Falato (2016), p. 551. Sul tema si rinvia allo studio di Caianiello (2014), p. 144.

[5] Si può parlare di un nuovo diritto fondamentale, quello alla «libertà informatica», secondo la definizione di Orlandi (2018), p. 541, il quale ritiene che lo stesso dovrebbe essere ricavato dall'art. 2 Cost.

[6] Nella dottrina costituzionalistica, l'art. 2 Cost. viene considerato alla stregua di una fattispecie aperta, fonte di nuovi diritti della personalità, cfr. Barbera (1975), p. 80. *Contra*, Barile (1984), p. 54, secondo cui l'art. 2 Cost. è «matrice e garante dei diritti di libertà, non fonte di altri diritti, al di là di quelli contenuti in Costituzione».

[7] In questo senso: Camon (2017a), p. 94; Felicioni (2016) p. 127 e Lasagni (2016), p. 14.

[8] Al riguardo, sono attuali le considerazioni di Grevi (1976), p. 2: «il diritto alla libertà personale, atteso il carattere peculiare e primordiale dell'interesse che vi è garantito, si configura nel sistema come presupposto di tutti gli altri diritti di libertà, in quanto logicamente li precede e li condiziona a livello operativo, rendendone possibile la piena esplicazione».

[9] C'è unanimità di vedute sul fatto che l'art. 13 Cost. intenda proteggere la libertà personale dalle coercizioni fisiche, mentre è dibattuta la possibilità che la norma si riferisca a profili ulteriori della libertà personale, che trascendono la dimensione prettamente fisica. Per una lettura restrittiva dell'art. 13 Cost. v. Amato (1967), p. 20; secondo Barbera (1967), p. 40, invece, il concetto di libertà personale dell'art. 13 Cost. comprende anche la libertà morale dell'individuo.

(come portafogli, portamonete, etc.) o ad immediato contatto con essa (come borse, borselli e borsette)» ([10]): a maggior ragione, l'estensione della garanzia dovrebbe oggi riguardare anche i dispositivi informatici mobili (quali ad esempio i telefoni cellulari di nuova generazione, *tablet*, *computer* portatili), odierne proiezioni della vita individuale sotto molteplici aspetti.

Intuitiva è anche la rilevanza, rispetto alla materia che qui si affronta, dell'art. 15 Cost. che, al comma 1, protegge la libertà della corrispondenza e di ogni altra forma di comunicazione e, al comma 2, prescrive che qualsiasi limitazione possa avvenire «soltanto per atto motivato dell'autorità giudiziaria e con le garanzie previste dalla legge». La disposizione, anche se ampia e in grado di proteggere ogni «collegamento della persona con il mondo esterno» ([11]), si rivela però insufficiente rispetto allo scopo di individuare il fondamento costituzionale di un nuovo diritto fondamentale, perché in grado di attrarre nella propria orbita di tutela solo una delle possibili modalità di impiego del captatore informatico, ossia quella di strumento di intercettazione.

Molti individuano la possibile fonte di protezione di questa nuova libertà fondamentale che si va consolidando nell'art. 14 Cost., ossia nel concetto di "domicilio informatico" inteso come un'area ancora più intima rispetto a quella inerente il comune domicilio fisico, già presidiato attraverso una doppia riserva di legge e di giurisdizione ([12]).

Anche in questo caso, pur essendo il richiamo tutt'altro che fuori luogo, l'impressione è che l'aggressione al c.d. domicilio informatico mediante l'utilizzo di un captatore possa persino travalicare i confini della tutela di uno spazio – fisico o immateriale che sia – e costituire una forma di intrusione più pervasiva, perché destinata a toccare sfere ancora più intime, legate al rispetto stesso della dignità umana.

Un ulteriore percorso finalizzato a riconoscere l'esistenza di una nuova libertà fondamentale, che abbia ad oggetto l'uso riservato dei sistemi informatici quale esplicazione della personalità umana, trova i propri referenti normativi nelle fonti sovranazionali. Nell'art. 7 della Carta dei diritti fondamentali dell'Unione europea, così come nell'art. 8 della Convenzione europea dei diritti dell'uomo, infatti, la tutela della riservatezza della vita privata e familiare assurge al rango di diritto fondamentale. Inoltre, l'art. 8 della Carta dei diritti fondamentali dell'Unione europea si occupa specificamente – e autonomamente rispetto alle norme da ultimo citate – della tutela dei dati di carattere personale ([13]).

La portata della tutela *multi-level* è variamente interpretata: ora come inadeguata rispetto alla dimensione della libertà informatica ([14]), ora come fonte da cui ricavare il riconoscimento di un nuovo diritto inviolabile ([15]).

In ultima analisi, non sembra profilarsi la necessità di una revisione costituzionale, che definisca in modo esplicito l'esistenza di un inedito diritto fondamentale, ampliando il catalogo del Titolo I della Parte I della Costituzione; piuttosto, un intervento della Corte costituzionale, con una presa di posizione analoga a quella tedesca, potrebbe riconsiderare i confini delle libertà fondamentali tradizionali, oggi esposte a nuove forme di potenziale compressione. In altre parole, la Corte potrebbe favorire un'estensione della tutela dell'individuo tenendo conto del fatto che ormai l'espressione della personalità passa attraverso l'uso dei sistemi informatici.

[10] Cfr. Corte cost., sent. n. 88/1987, richiamata da Camon (2017a), p. 95.
[11] Così Barile e Cheli (1962), p. 744.
[12] Così Camon (2017a), p. 95 e Parlato (2017), p. 302; secondo Caprioli (2017), p. 490, il domicilio informatico costituisce una «proiezione informatica dell'individuo, destinata ad allargare i confini del diritto all'intimità della vita privata e al rispetto della dignità personale». Con la legge 23 dicembre 1993, n. 547, è stato introdotto l'art. 615-*ter* c.p. (accesso abusivo ad un sistema informatico o telematico) tra i reati contro l'inviolabilità del domicilio e, in quell'occasione, si è ritenuto che «i sistemi informatici o telematici, la cui violazione essa reprime, costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 Cost.»: in questi termini la Relazione al disegno di legge C-2773. In dottrina si è giunti alla definizione di un «diritto all'intangibilità della vita digitale»: così Signorato (2018a), p. 69.
[13] Sull'art. 8 C.e.d.u., cfr. Cisterna (2016a), p. 215 e Balsamo (2017), p. 171. Per quanto riguarda la Carta dei diritti fondamentali dell'Unione Europea si rinvia ai commenti *sub* art. 7 di Martinico (2017), p. 116 e *sub* art. 8 di Pollicino e Bassini (2017), p. 134. Senza trascurare l'operatività della clausola di equivalenza dell'art. 52 della Carta dei diritti fondamentali dell'Unione Europea, in base alla quale «laddove la Carta contenga diritti corrispondenti a quelli garantiti dalla [C.e.d.u.], il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta Convenzione».
[14] In questo senso: Orlandi (2018), p. 542.
[15] Con accenti diversi: Iovene (2014), p. 338, sostiene che la riservatezza informatica possa essere ricondotta all'art. 7 della Carta dei diritti fondamentali dell'Unione Europea e non all'art. 8, in quanto la garanzia non riguarderebbe il controllo sulle modalità di trattamento dei propri dati personali, bensì la tutela della persona in una dimensione – quella informatica – in cui vari aspetti della sua vita «si sono tradotti in dati, suscettibili di trattamento informatico»; nello stesso senso: Felicioni (2016), p. 127. Secondo Falato (2014), p. 558, invece, il diritto fondamentale in gioco è meglio salvaguardato dalla previsione dell'art. 8 della Carta, come protezione dei dati individuali.

3. I tentativi di collocazione sistematica delle indagini svolte tramite il captatore informatico.

Il problema di cui si discute nasce dal fatto che nel codice di procedura penale manca una compiuta regolamentazione della materia. La lacuna ha dunque portato gli interpreti a verificare se le attività investigative esperibili tramite il captatore informatico possano essere riconducibili a mezzi di ricerca della prova già disciplinati dalla legge ([16]).

Alcune delle possibili funzioni del nuovo strumento d'indagine, in effetti, sembrano trovare copertura legislativa in taluni istituti processuali "tradizionali": è il caso delle intercettazioni di comunicazioni informatiche o telematiche (art. 266-*bis* c.p.p.), alla cui disciplina la giurisprudenza ha ricondotto la captazione tramite *virus* non solo delle conversazioni svolte su applicazioni di messaggistica istantanea, ma anche di *e-mail* ([17]).

Più problematico è l'inquadramento di quella modalità di investigazione che viene denominata "*perquisizione online*": l'espressione, ormai entrata nell'uso comune, è indubbiamente fuorviante, poiché si riferisce ad un'attività investigativa che coniuga alcune delle funzioni tipiche dei mezzi di ricerca della prova codificati con la possibilità di esperire operazioni inedite, le quali dunque non rientrano né nello schema della perquisizione tradizionale (art. 247 c.p.p.), né in quello della perquisizione informatica (art. 247, comma 1-*bis*, c.p.p.) ([18]).

Dall'analisi del modello legale tipico, infatti, emergono vistose differenze che non consentono di ricondurre le perquisizioni *online* all'omologa disciplina codicistica: quest'ultima, pur declinando la perquisizione quale atto "a sorpresa", la colloca nell'ambito di una relazione comunque esplicita tra individuo e autorità, fondata sul riconoscimento di garanzie difensive ed informative che, per ovvie ragioni, non possono essere replicate nell'attività investigativa svolta mediante un *virus* che, per definizione, opera in modo nascosto; inoltre, le perquisizioni ordinarie sono finalizzate alla ricerca del corpo del reato e/o delle cose pertinenti al reato in relazione ad un addebito preesistente, e non quindi all'acquisizione indiscriminata di dati ([19]).

Tra l'altro, come già sottolineato, l'apprensione di dati informatici non esaurisce affatto il novero dell'attività esperibili mediante il captatore informatico: in molte di esse il connotato dell'assoluta originalità si è rivelato tanto prevalente da indurre alcuni a prospettare il ricorso alla categoria della "prova atipica" (art. 189 c.p.p.) ([20]).

Come noto l'istituto stabilisce che, per l'ingresso processuale di una prova che non trova corrispondenze codicistiche, è necessaria la verifica del rispetto di tre condizioni: che la prova in questione sia «idonea ad assicurare l'accertamento dei fatti»; che la sua assunzione non pregiudichi «la libertà morale della persona»; e infine che, prima di procedere all'ammissione della prova, il giudice senta «le parti sulle modalità di assunzione» ([21]).

Apparentemente, dunque, si potrebbe sostenere che il captatore informatico sia ammissibile come prova atipica, anche se il suo utilizzo non è regolato dalla legge ([22]). Tuttavia, l'art.

[16] La *summa divisio* tra le attività di c.d. "*online search*" e quelle di c.d. "*online surveillance*" è ben spiegata da Torre (2015), p. 1163. Alla prima categoria sono riconducibili quelle funzioni che permettono di fare la copia delle unità di memoria contenute nel dispositivo dell'apparecchio infettato; nella seconda, ad essere captato è il flusso di informazioni che va dalle unità periferiche (tastiera, videocamera, microfono, *etc.*) al microprocessore del dispositivo, consentendo un controllo in tempo reale completo.

[17] Sul punto v. Mancuso (2014), p. 66. In giurisprudenza, v. Cass., sez. IV, 28 giugno 2016, Boemio, in *C.E.D. Cass.* n. 268228: nel caso di specie la Corte ha ritenuto che le *e-mail* ricevute o inviate possano essere oggetto di intercettazione; non è così per le *e-mail* salvate nelle "bozze" e non inviate: queste ultime possono essere acquisite tramite un sequestro di dati informatici. In senso critico: Giordano (2017), il quale osserva che, nella decisione di cui si tratta, la Corte ha dato una giustificazione dell'impiego del *virus trojan* non condivisibile (vale a dire: «l'uso del *trojan* è stato limitato all'acquisizione della *password* di accesso agli *account* di posta elettronica», di conseguenza «si è usato il programma come si è da sempre usata la microspia»).

[18] Sull'ipotesi di ricondurre la perquisizione *online* allo schema legale dell'art. 247, comma 1-*bis*, c.p.p., così come modificato dalla l. 18 marzo 2008, n. 48, che ha ratificato la Convenzione di Budapest, v. Bontempelli (2018), p. 12. La norma in realtà si limita a legalizzare la perquisizione in ambito informatico o telematico «quando vi è motivo di ritenere che ivi si trovino dati, informazioni, programmi informatici o tracce comunque pertinenti al reato»: lo schema rimane quello di un atto "a sorpresa", ma esso non viene effettuato in modo occulto, bensì con le garanzie già previste per le perquisizioni "tradizionali". Analogo discorso vale per l'inapplicabilità delle disposizioni sulle ispezioni informatiche, anch'esse novellate nel 2008.

[19] Rimarcano le differenze con la perquisizione "tradizionale": Marcolini (2010), p. 2858; Caprioli (2017), p. 489 e Trogu (2014), p. 444.

[20] La giurisprudenza ha fatto ricorso alla prova atipica in più di un'occasione in questa materia. Cfr. Cass., sez. V, 14 ottobre 2009, Virruso, in *C.E.D. Cass.* n. 246954, nonché, recentemente Cass., sez. V, 30 maggio 2017, in *C.E.D. Cass.* n. 271412. In generale, in tema di prova atipica si rinvia alla riflessione di Nobili (1990), p. 398. Sulla possibile riforma dell'art. 189 c.p.p., v. le interessanti conclusioni di Camon (2017b) p. 425.

[21] In dottrina si è discusso se la disciplina dell'art. 189 c.p.p. potesse essere riferita anche ai mezzi di ricerca della prova, con la peculiarità che, in tal caso, il contraddittorio non potrebbe essere anticipato ma postumo. Sul tema, v. anche Signorato (2018a), p. 256.

[22] Dubbi sulla possibile lesione della libertà morale del possessore inconsapevole di un dispositivo infettato sono espressi da Bontempelli

189 c.p.p. incontra un limite invalicabile, ossia quello della potenziale limitazione delle libertà che la Costituzione ritiene inviolabili: in questo ambito non vi è spazio per investigazioni atipiche, ma occorre che sia la legge ordinaria a stabilire con precisione in quali casi, con quali modalità e con quali garanzie le libertà fondamentali possano essere limitate. Fuori da tali ipotesi, la prova è vietata e, se acquisita, è inutilizzabile perché incostituzionale ([23]).

In assenza di una presa di posizione chiara da parte del legislatore ([24]), lo schema della sussumibilità del captatore talora entro i confini di un istituto disciplinato dal codice, talora nell'ambito della prova atipica, non solo non pare essere risolutivo, ma contribuisce ad innalzare il tasso di discrezionalità applicativa e mette in crisi la stessa legalità del sistema processuale ([25]).

4. I contenuti del recente intervento legislativo.

Se è vera la premessa di partenza, ossia che le nuove indagini tecnologiche sono potenzialmente in grado di comprimere in modi sinora sconosciuti alcuni diritti fondamentali, allora non si può che considerare insoddisfacente la recente riforma che introduce e disciplina l'uso dei captatori informatici ([26]).

Senza dubbio, infatti, la potenzialità intrusiva e la versatilità dello strumento avrebbero richiesto una regolamentazione adeguata alle molteplici insidie che possono derivare dal suo impiego: la legge invece si è concentrata solo su uno dei possibili fini investigativi, ossia l'intercettazione di comunicazioni tra presenti ([27]), e ha lasciato alla giurisprudenza il delicato compito di selezionare, tra le possibili funzioni, quelle consentite e quelle inammissibili.

È possibile che il *self restraint* del legislatore sia stato indotto dai contenuti di alcune sentenze della Corte di cassazione rese in argomento, ed in particolare dalla pronuncia delle sezioni unite che, correttamente, aveva contenuto l'ambito del proprio decidere al quesito posto dalla sezione rimettente, che riguardava l'utilizzabilità del captatore informatico nei luoghi di privata dimora ([28]). Anche se si è ormai abituati ad un legislatore che positivizza, o che, quantomeno, utilizza alla stregua di proposte di legge le decisioni del Supremo Collegio, sembra comunque discutibile la scelta di aver considerato meritevole di tutela il solo diritto fondamentale inerente alla libertà ed alla segretezza delle comunicazioni in ambito domiciliare. Le tecnologie informatiche oggi in uso consentono intrusioni che vanno ben oltre l'ambito dell'art. 15 Cost., ragione questa che avrebbe dovuto ispirare scelte legislative diverse e nettamente più puntuali.

A ben vedere, nella nuova disciplina si scorge un doppio limite: il captatore può essere utilizzato solo come mezzo di intercettazione ambientale e solo su dispositivi portatili. Dall'analisi di entrambi i limiti, per ragioni diverse, emergono numerose perplessità.

(2018), p. 14, e da Signorato (2018a), p. 238, che intravede una possibile violazione del «principio del *nemo tenetur se detegere*, da intendersi in senso ampio, non solo come diritto a non rendere dichiarazioni autoincriminanti, ma anche come diritto a non compiere azioni autoincriminanti». *Contra*, Caprioli (2017), p. 486 e Torre (2017), p. 69, il quale ritiene che il carattere occulto del captatore assicura «l'integrità del processo volitivo della persona».

[23] La Corte di cassazione ha stabilito che l'art. 189 c.p.p. «presuppone logicamente la formazione lecita della prova» e che quindi nel caso delle attività atipiche il vaglio di ammissibilità è preliminare rispetto a quello di utilizzabilità, v. in tema di videoriprese, Cass., sez. un., 28 marzo 2006, Prisco, in *Cass. pen*., 2006, p. 3943, con note di Di Bitonto (2006) e Ruggieri (2006), p. 3937. Secondo un autorevole ragionamento dottrinale, invece, fino alla declaratoria di illegittimità costituzionale dell'art. 189 c.p.p., le prove atipiche sarebbero da considerare ammissibili, così Cordero (2003), p. 848. In argomento, v. anche Daniele (2013), p. 367, secondo cui sebbene i requisiti di ammissibilità *ex* 189 c.p.p. siano generici, da ciò non potrebbe ricavarsi l'inutilizzabilità delle prove ottenute, bensì la necessità di sollevare una questione di legittimità costituzionale della previsione di cui all'art. 189 c.p.p.

[24] Ha invocato l'inserimento nel codice di procedura penale di un capo dal titolo «Atto di indagine non disciplinato dalla legge che incide su un diritto fondamentale della persona», Marcolini (2015), p. 760.

[25] Del resto, basterebbe considerare che la prova atipica «non ha la funzione di aprire il sistema, bensì di chiuderlo»: Conti (2018), p. 1211.

[26] La disciplina di recente introduzione appare deludente anche in rapporto ad altre precedenti proposte di legge in tema di captatore informatico. Tra di esse, vale la pena di evidenziare che la n. C. 3762 del 20 aprile 2016, dal titolo «Disciplina dell'uso dei captatori legali nell'ambito delle garanzie individuali"», promossa dal deputato Quintarelli, coglieva con maggiore precisione tecnica il potenziale dello strumento, e prevedeva l'introduzione dell'art. 254-*ter* c.p.p., come nuovo mezzo di ricerca della prova denominato «osservazione e acquisizione da remoto».

[27] Questo è il vero limite dell'intervento legislativo secondo Curtotti e Nocerino (2018), p. 544 e Bronzo (2018), p. 237; secondo Rivello (2018) p. 119, invece, la scelta legislativa sarebbe un'attuazione del principio di proporzionalità.

[28] Il riferimento è a Cass., sez. un., 26 aprile 2016, Scurato, in *Arch. n. proc. pen*., 2017, p. 76 con nota di Camon (2017a), p. 91. Per alcuni commenti alla decisione si rinvia a Capone (2017), p. 1263; Cisterna (2016b), p. 331; Corasaniti (2016), p. 88; Gaito e Furfaro (2016), p. 309; Lasagni (2016), p. 1; Nocerino (2016), p. 3565; Testaguzza (2016), p. 1. Sulla giurisprudenza, nazionale e sovranazionale, in tema di captatore informatico, si rinvia a Balsamo (2016), p. 2274.

Da un lato, infatti, la mancata previsione legislativa di usi diversi da quello appena ricordato (per esempio, le perquisizioni *online*) lascia intendere che essi non siano consentiti. Il punto non è secondario: anzi, come si è visto, il vuoto legislativo crea grandi incertezze applicative ([29]).

Dall'altro lato, non è chiara la ragione della scelta di delimitare l'intercettazione tramite captatore ai soli apparecchi portatili (*smartphone*, *tablet*, *pc* portatili ma non quelli fissi anche se connessi ad *internet*): dal punto di vista del risultato investigativo ottenibile, così come da quello delle possibili compressioni di diritti individuali, non si scorge alcuna differenza tra la captazioni in un apparecchio mobile e quella disposta in uno fisso; peraltro, trattandosi di un limite che il legislatore ha dettato in modo esplicito, poche *chances* residuano per l'ipotesi che si tratti di una svista. *Rebus sic stantibus*, le intercettazioni tramite captatore disposte su un dispositivo fisso potrebbero essere ricondotte in via interpretativa solo alla disciplina delle intercettazioni telematiche di cui all'art. 266-*bis* c.p.p..

Anticipato dalla delega contenuta nella legge n. 103/2017, che dettava principi assai stringenti ([30]), sul finire della scorsa legislatura è stato emanato il d.lgs. 29 dicembre 2017, n. 216 che ha modificato, integrandoli, gli artt. 266 e ss. c.p.p..

Con una replica non proprio fedele all'originale dei principi dettati dalle sezioni unite nella decisione Scurato sopra richiamata, la dimensione applicativa del captatore informatico viene diversificata a seconda della tipologia di reato da accertare. Infatti, per tutti i delitti per cui sono ammesse le intercettazioni (art. 266, c. 1, c.p.p.), lo strumento può essere utilizzato per captare conversazioni sia *extra*, sia *infra*-domiciliari, ma queste ultime sono legittime solo nel caso in cui vi sia fondato motivo di ritenere che nel domicilio sia in corso l'attività criminosa.

Invece, l'intercettazione tramite captatore è sempre consentita – anche nei luoghi di privata dimora – nell'ambito dei procedimenti per i delitti di cui all'art. 51 commi 3-*bis* e 3-*quater*, rispetto ai quali la presunzione di continuità della condotta criminale deriva dalla particolare gravità dei reati inclusi negli elenchi degli articoli appena menzionati ([31]).

Attraverso la distinzione tra luoghi operata dalla legge si creano dunque statuti di protezione differenziati nei confronti dello stesso atto di indagine, giustificati dalla maggiore gravità, o meglio dal vero e proprio allarme sociale, che connota i reati di criminalità organizzata ([32]).

La maggiore invasività del captatore informatico rispetto ai tradizionali strumenti di intercettazione non è sfuggita al legislatore, che ha introdotto una previsione che sembra imporre al giudice di vagliare la richiesta del pubblico ministero alla luce del principio di proporzionalità. Infatti, l'art. 267, comma 1, c.p.p. prevede che il giudice indichi, nel decreto autorizzativo, "le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini". La previsione si aggiunge al testo della prima parte del comma 1 dell'art. 267 c.p.p., che già prevedeva il ricorso all'intercettazione nei casi di «assoluta indispensabilità» (ovvero allorquando altri mezzi di ricerca della prova - meno invasivi - non risultassero esperibili); la novella, con il riferimento alla «necessità» dell'intercettazione tramite captatore, rende eccezionale questa tipologia anche rispetto alle intercettazioni ambientali tradizionali.

La previsione legislativa pare opportuna nella prospettiva di rafforzare l'onere motivazionale per l'impiego del *virus* informatico, attesa la maggiore intrusività nella sfera di riservatezza del soggetto sottoposto al controllo. Cionondimeno è possibile che, nella prassi applicativa, questo presupposto tenderà a sfumare e che si finirà per estendere le maglie autorizzative delle

[29] Condivisibilmente, Bronzo (2018), p. 239 segnala che il captatore può svolgere funzioni contigue, dunque non è difficile che da una si possa trasmodare nell'altra senza che possa essere garantito un preventivo controllo da parte del pubblico ministero o della polizia giudiziaria.
[30] Per un commento alla delega di cui all'art. 1, commi 82, 83 e 84, lett. *a*, *b*, *c*, *d* ed *e* della legge n. 103 del 2017, v. Lonati (2017), p. 61 e Turco (2017), p. 316.
[31] Viene mantenuta, ma molto ridimensionata, l'idea di un doppio binario applicativo. Le sezioni unite, infatti, avevano ritenuto che l'impiego del *trojan* fosse ammissibile anche nei luoghi di privata dimora per i procedimenti concernenti reati di criminalità organizzata, avallando al riguardo una nozione molto ampia di «delitti di criminalità organizzata», cfr. Giordano (2018), p. 256. Viceversa, sulla scorta della considerazione per cui la sanzione processuale dell'inutilizzabilità non è sufficiente a colmare la lesione di un diritto fondamentale, nella decisione veniva escluso l'impiego dei captatori per i reati ordinari, cioè quelli rientranti nell'ambito della disciplina di cui al comma 2 dell'art. 266 c.p.p., dal momento che non è prevedibile *ex ante* la movimentazione dell'apparecchio e dunque il possibile utilizzo dentro i luoghi di privata dimora. Secondo la lettura di Cajani (2016), p. 4140, l'utilizzo del captatore per i reati comuni, in luoghi diversi da quelli di privata dimora, invece, sarebbe da ritenere ammissibile, purché tali luoghi siano stati previamente indicati nella richiesta di autorizzazione all'intercettazione.
[32] La legge equipara, in materia di uso dei captatori, la disciplina dei più gravi reati commessi dai pubblici ufficiali contro la pubblica amministrazione – vale a dire quelli puniti con la pena della reclusione non inferiore nel massimo a cinque anni – a quella dettata per i reati di criminalità organizzata e terrorismo, prevedendo che per i reati appartenenti alla prima categoria si applichino le disposizioni di cui all'art. 13, d.l. n. 152 del 1991. Sul punto, v. Varraso (2018), p. 148.

intercettazioni ambientali con captatore informatico, senza previamente esaminare la loro necessità in rapporto alla modalità tradizionale.

Sempre con riguardo al decreto autorizzativo, per i reati diversi da quelli di cui all'art. 51, commi 3-*bis* e 3-*quater*, c.p.p., la medesima norma impone di indicare "i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono", dando conto del fatto che il legislatore ha concepito il captatore come uno strumento che agisce sì in modo itinerante, ma non ininterrotto. Per azionare il funzionamento del *virus*-spia, infatti, è necessario avviare da remoto un apposito comando, e le relative operazioni sono espletate dalla polizia giudiziaria che, secondo quanto disposto dalla seconda parte dell'art. 268, comma 3-*bis*, c.p.p., può avvalersi di persone idonee a collaborare, perché dotate delle competenze tecniche, ai sensi dell'art. 348, comma 4, c.p.p..

La predeterminazione – anche indiretta ([33]) – dei luoghi dell'intercettazione secondo una sorta di "progetto d'indagine", in grado di evidenziare la relazione tra mezzo di indagine e risultato atteso, è una previsione che pare essere confacente allo scopo "sulla carta", ma estremamente complessa sul piano concreto.

A parte la considerazione che un'attività captativa ad intermittenza, oltre che assai dispendiosa e tecnicamente incerta ([34]), rischierebbe di compromettere il connotato occulto dell'indagine (per esempio, causando cali repentini della carica dell'apparecchio infettato e dunque svelando al soggetto controllato la presenza del *virus*), a preoccupare è soprattutto il rischio che ci si rassegni ad una prassi di decreti autorizzativi dal contenuto volutamente vago, tenuto conto che difficilmente l'autorità giudiziaria potrà prevedere *ex ante* gli sviluppi investigativi e dunque il preciso raggio d'azione necessario per predisporre una captazione efficace ([35]).

In generale, non è consentito al pubblico ministero di disporre, con proprio decreto, le intercettazioni di comunicazioni tra presenti mediante captatore informatico, fatti salvi i casi per cui si proceda per i reati di cui all'art. 51, comma 3-*bis* e 3-*quater*, c.p.p.: è quello che stabilisce il nuovo comma 2-*bis* dell'art. 267 c.p.p.[]. Il decreto urgente, emesso nei casi in cui vi sia il fondato timore di ritenere che dal ritardo possa derivare un grave pregiudizio alle indagini, sarà oggetto della convalida del giudice nelle quarantotto ore successive e dovrà dare conto anche delle ragioni che rendono impossibile attendere il provvedimento del giudice.

Interessanti sono infine i limiti di utilizzabilità posti dal legislatore. Il primo, quello previsto all'art. 270, c. 1-*bis*, c.p.p. vieta l'uso dei dati acquisiti con captatore per provare la sussistenza di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione. Si nota subito la differenza rispetto al comma 1 dello stesso articolo dove è previsto un analogo divieto con riguardo non a reati diversi, bensì a procedimenti diversi da quelli nei quali l'intercettazione è stata disposta ([36]). Il comma 1-*bis* riguarda invece sia la trasmigrazione da un procedimento ad un altro, sia l'uso della stessa prova all'interno del medesimo procedimento. Il divieto è stato introdotto allo scopo di arginare possibili "trucchi" sulla qualificazione giuridica dei reati, posti in essere proprio per ottenere autorizzazioni indebite: se nel decreto autorizzativo si attribuisse al delitto una qualifica che ammette l'intercettazione con captatore, i dati acquisiti sarebbero inutilizzabili nei confronti dell'imputato qualora l'addebito venisse poi derubricato a reato che non ammette la captazione ([37]).

La seconda previsione che detta limiti di utilizzabilità è riportata al comma 1-*bis* dell'art. 271, e stabilisce che "non sono in ogni caso utilizzabili i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico e i dati acquisiti al di fuori del limite di tempo e di luogo indicati nel decreto autorizzativo". Nelle intenzioni legislative, dunque, al fine di accrescere la tutela delle prerogative individuali parrebbe delinearsi l'idea di un inizio ufficiale per questo tipo di intercettazione ambientale che deve risultare da verbale e che esclu-

[33] Il decreto di autorizzazione potrebbe dunque essere motivato facendo ricorso ad espressioni del tipo «ogni volta che si rechi nel locale y», «ovunque incontri il soggetto x».

[34] L'attuale tecnologia di funzionamento dei *virus* non sembra in linea con la previsione di legge. I captatori non consentono sempre un ascolto simultaneo della conversazione intercettata, bensì acquisiscono i dati digitali nei quali essa viene tradotta: lo spiega Bronzo (2018), p. 251, il quale sottolinea l'esistenza di un «notevole margine di errore».

[35] Ed è nota la tendenza giurisprudenziale, registrata in materia di intercettazioni telefoniche, al contenimento motivazionale del decreto autorizzativo. Cfr., ad esempio, Cass., sez. V, 27 maggio 2004, Scardamaglia, in *Guida dir.*, 2004, n. 26, p. 76.

[36] Quello previsto dal comma 1 dell'art. 270 c.p.p. è un divieto dalla portata più ridotta e che costituisce una sorta di appendice dell'art. 238 c.p.p. secondo Orlandi (2018), p. 550.

[37] La norma è tanto opportuna da pensare che il limite debba essere esteso a tutte le forme di intercettazione: di questo avviso Camon (1996), p. 263, con riguardo alle intercettazioni "tradizionali".

de quanto registrato durante le attività preliminari ([38]).

5. Le modalità esecutive della nuova forma di intercettazione ambientale.

Le regole sugli accorgimenti di carattere tecnico, che sostanzialmente riguardano le modalità di esecuzione delle attività di intercettazione, sono contenute nell'art. 89 disp. att. c.p.p. ([39]). Innanzitutto, la legge prevede che possano essere impiegati solo «programmi conformi ai requisiti tecnici stabiliti con decreto del Ministro della giustizia» (comma 2-*bis*), e che il verbale debba indicare il tipo di programma utilizzato e i luoghi in cui si svolgono le comunicazioni o le conversazioni (comma 1), così da consentire alla difesa una verifica sul rispetto dei limiti previsti nel decreto di autorizzazione.

Anche le successive disposizioni rimarcano l'attenzione legislativa a che sia operato un controllo sulla sicurezza delle operazioni: è a tale scopo, infatti, che il prodotto dell'attività di intercettazione dovrà essere trasferito verso gli impianti della procura della Repubblica, avendosi cura di precisare nel verbale le condizioni tecniche di sicurezza e affidabilità della rete di trasmissione e assicurando che quanto intercettato sia integralmente corrispondente al testo trasmesso. Ove risulti impossibile l'immediato trasferimento dei dati, il verbale deve indicare le ragioni che hanno ostacolato la contestuale trasmissione. Una volta concluse queste operazioni, il captatore dovrà necessariamente essere disattivato, affinché ne sia inibito l'uso successivo ([40]).

Un decreto del Ministero della Giustizia del 30 aprile 2018 indica i requisiti tecnici che i programmi informatici devono avere: non c'è bisogno di essere esperti di tecnologie informatiche per capire che si tratta di indicazioni inadeguate perché molto generiche, inevitabilmente destinate a produrre controversie sull'affidabilità dei risultati investigativi ([41]).

6. Brevi osservazioni conclusive.

Nell'estrema limitatezza dell'intervento legislativo, si può concludere affermando che usi del captatore informatico diversi da quelli che sono oggi espressamente regolati dal codice non sono ammessi: ad impedirlo è l'emersione di un diritto fondamentale che protegge l'utilizzo libero dei sistemi informatici. Solo il suo riconoscimento farà da *enforcement* per il legislatore, che dovrà regolamentare l'impiego del captatore informatico a fini d'indagine facendo riferimento alla procedura richiesta dalla Costituzione per la limitazione di un diritto fondamentale, ossia riserva di legge e di giurisdizione, alla luce di un bilanciamento tra esigenze di segno opposto (quella dell'accertamento e repressione dei reati e quella al pieno godimento dei diritti individuali) che deve essere operato secondo il principio di proporzionalità. Solo questo passaggio potrà impedire di leggere i vuoti legislativi come assenza di qualsiasi divieto nell'uso del captatore come mezzo di controllo o di perquisizione a distanza.

L'introduzione della disciplina, come noto, è al momento "congelata": dopo un primo rinvio al 31 marzo 2019 ad opera del d.lgs. 91/2018, la legge di Bilancio 2019 ha rimandato per la seconda volta l'entrata in vigore della riforma ([42]). Le norme si applicheranno dunque alle operazioni relative a provvedimenti autorizzativi emessi dopo il 31 luglio 2019, al dichiarato

[38] Dubbi sull'utilità della clausola sono espressi da Giordano (2018), p. 275 e Orlandi (2018), p. 551: dato che l'inserimento del *virus* nell'apparecchio bersaglio non può precedere l'autorizzazione del G.i.p., non è chiaro quali siano le «operazioni preliminari» cui allude la norma che non siano già coperte dal generale divieto di utilizzabilità di intercettazioni svolte in assenza di autorizzazione. Stesse perplessità sono state sollevate anche dal Garante per la protezione dei dati personali, con il parere reso in data 2 novembre 2017 sullo schema di decreto legislativo del Governo.

[39] Una collocazione, quella tra le disposizioni d'attuazione del codice di rito, che non corrisponde all'importanza delle previsioni ivi contenute, v. Orlandi (2018), p. 548.

[40] Sulle modalità operative dell'attività captativa, cfr. diffusamente Signorato (2018b), p. 263.

[41] Si tratta del D.M. 20 aprile 2018 recante "Disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'art. 7, commi 1 e 3 del decreto legislativo 29 dicembre 2017, n. 216". Al riguardo si rinvia a Torre (2018), p. 1255 e Ziccardi (2018) p. 479.

[42] Legge n. 145/2018, in G.U. n. 302 del 31 dicembre 2018, suppl. ord. n. 62: in particolare, l'art. 1, comma 1139, lett. *a)* ha modificato l'art. 9, comma 1, d.lgs. 216/2017 sostituendo alle parole «dopo il 31 marzo 2019», le parole «dopo il 31 luglio 2019».

scopo di adeguare le procure alle nuove tecnologie, ma, si spera, anche a quello di rimeditare nel complesso la regolamentazione dell'utilizzo dei captatori informatici.

Bibliografia:

Amato, Giuliano (1967): *Individuo e autorità nella disciplina della libertà personale* (Milano, Giuffrè)

Balsamo, Antonio (2016): "Le intercettazioni mediante *virus* informatico tra processo penale italiano e Corte europea", *Cassazione penale*, pp. 2274-2288

Balsamo, Antonio (2017): "Il contenuto dei diritti fondamentali", in Kostoris, Roberto E. (a cura di): *Manuale di procedura penale europea* (Milano, Giuffrè), pp. 115-195

Barbera, Augusto (1967): *I principi costituzionali della libertà personale* (Milano, Giuffrè)

Barbera, Augusto (1975): "Commento all'art. 2", in Branca, Giuseppe (a cura di): *Commentario alla Costituzione. Artt. 1-12. Principi fondamentali* (Bologna, Zanichelli), pp. 50-122

Barile, Paolo e Cheli, Enzo (1962): "Voce «Corrispondenza (Libertà di)», *Enciclopedia del diritto*, (Milano, Giuffrè), pp. 743-753

Barile, Paolo (1984): *Diritti dell'uomo e libertà fondamentali* (Bologna, Il Mulino)

Bontempelli, Manfredi (2018): "Il captatore informatico in attesa della riforma", *Diritto penale contemporaneo*, 20 dicembre 2018

Brighi, Raffaella (2018): "Funzionamento e potenzialità investigative del *malware*", in Giostra, Glauco e Orlandi, Renzo (a cura di): *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche* (Torino, Giappichelli), pp. 211-233

Bronzo, Pasquale (2018): "Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori", in Giostra, Glauco e Orlandi, Renzo (a cura di): *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche* (Torino, Giappichelli), pp. 236-262

Caianiello, Michele (2014): "Il principio di proporzionalità nel processo penale", *Diritto penale contemporaneo – Rivista trimestrale*, 3-4, pp. 143-163

Cajani, Francesco (2016): "Odissea del captatore informatico", *Cassazione penale*, pp. 4139-4151

Camon, Alberto (1996): *Le intercettazioni nel processo penale* (Milano, Giuffrè)

Camon, Alberto (2017a): "Cavalli di Troia in Cassazione", *Archivio della nuova procedura penale*, pp. 91-100

Camon, Alberto (2017b): "La fase che "non conta e non pesa". Indagini governate dalla legge?", *Diritto penale e processo*, pp. 425-434

Capone, Arturo (2017): "Intercettazioni e Costituzione. Problemi vecchi e nuovi", *Cassazione penale*, pp. 1263-1276

Caprioli, Francesco (2017): "Il captatore informatico come strumento di ricerca della prova in Italia", *Revista brasileira de Direito Processual Penal*, pp. 483-510

Cisterna, Alberto (2016a): "Cedu e diritto alla privacy", in Gaito, Alfredo (a cura di): *I principi europei del processo penale* (Roma, Dike), pp. 193-268

Cisterna, Alberto (2016b): "Spazio ed intercettazioni, una *liason* tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite", *Archivio penale*, pp. 331-347

Conti, Carlotta (2018): "Prova informatica e diritti fondamentali: a proposito di captatore e non solo", *Diritto penale e processo*, pp. 1210-1221

Corasaniti, Giuseppe (2016): "Le intercettazioni "ubiquitarie" e digitali tra garanzie di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali", *Il diritto dell'informazione e dell'informatica*, pp. 88-103

Cordero, Franco (2003): *Procedura penale* (Milano, Giuffrè)

Curtotti, Donatella e Nocerino, Wanda (2018): "Le intercettazioni tra presenti con captatore informatico", in Baccari, Gian Marco, Bonzano, Carlo, La Regina, Katia, Mancuso, Enrico M. (a cura di): *Le recenti riforme in materia penale* (Cedam, Milano), pp. 557-586

Daniele, Marcello (2013): "Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?", *Cassazione penale*, pp. 367-375

Di Bitonto, Maria Lucia (2006): "Le riprese video domiciliari al vaglio delle Sezioni Unite", *Cassazione penale*, pp. 3950-3962

Falato, Fabiana (2016): "L'uso (preventivo e repressivo) di dati personali come compressione di un diritto inviolabile", *Giustizia penale*, pp. 548-571

Felicioni, Paola (2015): *Le ispezioni e le perquisizioni* (Milano, Giuffrè)

Felicioni, Paola (2016): "L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma", *Processo penale e giustizia*, pp. 118-138

Filippi, Leonardo (2016): "L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico), *Archivio penale*, 2016, pp. 348-353

Flor, Roberto (2009): "Brevi riflessioni a margine della sentenza del *Bundesverfassungsgericht* sulla c.d. *online durchsuchung*. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona", *Rivista trimestrale diritto penale dell'economia*, pp. 695-716

Gaito, Alfredo e Fùrfaro, Sandro (2016): "Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività", *Archivio penale*, pp. 309-330

Giordano, Luigi (2017): "Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo", *Diritto penale contemporaneo*, 3, pp. 177-195

Giordano, Luigi (2018): "La disciplina del "captatore informatico"", in Bene, Teresa (a cura di): *L'intercettazione di comunicazioni* (Cacucci, Bari), pp. 247-285

Grevi, Vittorio (1976): *Libertà personale dell'imputato e Costituzione* (Milano, Giuffrè)

Iovene, Federica (2014): "Le c.d. perquisizioni *online* tra nuovi diritti fondamentali ed esigenze di accertamento penale", *Diritto penale contemporaneo – Rivista trimestrale*, 3-4, pp. 329-342

Lasagni, Giulia (2016): "L'uso di captatori informatici ("*trojans*") nelle intercettazioni "tra presenti"", *Diritto penale contemporaneo*, 7 ottobre 2016

Lonati, Simone (2017): "Sulla delega in materia di intercettazioni di conversazioni o comunicazioni", *Archivio nuova procedura penale*, pp. 58-66

Mancuso, Enrico M. (2014): "L'acquisizione di contenuti *e-mail*", in Scalfati, Adolfo (a cura di): *Le indagini atipiche* (Torino, Giappichelli), pp. 53-86

Marcolini, Stefano (2010): "Le cosiddette perquisizioni *on-line* (o perquisizioni elettroniche)", *Cassazione penale*, pp. 2855-2868

Marcolini, Stefano (2015): "Le indagini atipiche a contenuto tecnologico nel processo penale", in *Cassazione penale*, pp. 760-792

Martinico, Giuseppe (2017): "Art. 7. Rispetto della vita privata e della vita familiare", in Mastroianni Roberto, Pollicino, Oreste, Allegrezza, Silvia, Pappalardo, Fabio, Razzolini, Orsola (a cura di): *Carta dei diritti fondamentali dell'Unione Europea* (Milano, Giuffrè), pp. 116-133

Nicolicchia, Fabio (2017): "I limiti fissati dalla Corte costituzionale tedesca agli strumenti di controllo tecnologico occulto: spunti per una trasposizione nell'ordinamento italiano", in *Archivio penale* (rivista web), pp. 1-14

Nobili, Massimo (1990): "Art. 189 c.p.p.", Chiavario, Mario (a cura di): "Commento al nuovo codice di procedura penale", vol. II (Torino, Utet), pp. 397-402

Nocerino, Wanda (2016): "Le sezioni unite risolvono l'enigma: l'utilizzabilità del "captatore informatico" nel processo penale", *Cassazione penale*, pp. 3565-3584

Orlandi, Renzo (2014): "La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti individuali", *Rivista italiana di diritto e procedura penale*, 1996, pp. 1133-1164

Orlandi, Renzo (2018): "Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma", *Rivista italiana diritto e procedura penale*, pp. 538-556

Parlato, Lucia (2018): "Problemi insoluti: le perquisizioni *on-line*", in Giostra, Glauco e Orlandi, Renzo (a cura di): *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche* (Torino, Giappichelli), pp. 289-323

Pollicino, Oreste e Bassini, Marco (2017): "Art. 8. Protezione dei dati di carattere personale", in Mastroianni Roberto, Pollicino, Oreste, Allegrezza, Silvia, Pappalardo, Fabio, Razzolini, Orsola (a cura di): *Carta dei diritti fondamentali dell'Unione Europea* (Milano, Giuffrè), pp. 134-165

Rivello, Pierpaolo (2018): "Le intercettazioni mediante captatore informatico", in Mazza, Oliviero (a cura di): *Le nuove intercettazioni*, (Giappichelli, Torino), pp. 101-137

Ruggieri, Francesca (2006): "Riprese visive e inammissibilità della prova", *Cassazione penale*, pp. 3937-3949

Signorato, Silvia (2018a): *Le indagini digitali. Profili strutturali di una metamorfosi investigativa* (Torino, Giappichelli)

Signorato, Silvia (2018b): "Modalità procedimentali dell'intercettazione tramite captatore informatico", in Giostra, Glauco e Orlandi, Renzo (a cura di): *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, (Torino, Giappichelli), pp. 263-275

Testaguzza, Alessandra (2016): "*Exitus acta probant*. "*Trojan*" di Stato: la composizione di un conflitto", *Archivio penale* (rivista web), pp. 1-9

Torre, Marco (2015): "Il *virus* di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali", *Diritto penale e processo*, pp. 1163-1172

Torre, Marco (2017): *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali* (Milano, Giuffrè)

Torre, Marco (2018): "D.M. 20 aprile 2018: le disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico", *Diritto penale e processo*, pp- 1255-1258

Trogu, Mauro (2014): "Sorveglianza e "perquisizioni" *online* su materiale informatico", Scalfati, Adolfo (a cura di): *Le indagini atipiche* (Torino, Giappichelli), pp. 431-458

Turco, Elga (2017): "La ricerca della prova ad alta efficacia intrusiva: il captatore informatico", in Scalfati, Adolfo (a cura di): *La riforma della giustizia penale. Commento alla legge 23 giugno 2017, n. 103*, (Torino, Giappichelli), pp. 307-324

Varraso, Gianluca (2018): "Le intercettazioni e i regimi processuali differenziati per i reati di "grande criminalità" e per i delitti dei pubblici ufficiali contro la pubblica amministrazione, in Mazza, Oliviero (a cura di): *Le nuove intercettazioni*, (Giappichelli, Torino), pp. 139-160

Venegoni, Andrea e Giordano, Luigi (2016): "La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici", *Diritto penale contemporaneo.it,* 8 maggio 2016

Ziccardi, Giovanni (2018): "Il captatore informatico nella "Riforma Orlando": alcune riflessioni informatico-giuridiche", *Archivio penale*, pp. 479-511

Il controllo occulto e continuativo come categoria probatoria: premesse teoriche di una sistematizzazione

El control oculto y continuado como categoría probatoria: premisas teóricas de una sistematización

The Hidden and Continous Control as Evidentiary Notion: Theoretical Premises for a Systematic Analysis

Fabio Nicolicchia
Assegnista di ricerca presso l'Università degli Studi di Ferrara
nclfba@unife.it

Diritti fondamentali, Intercettazioni
Derechos fundamentales, Interceptación de comunicaciones
Fundamental rights, Intrusive surveillance

Abstracts

Lo scritto analizza il tema del ricorso a nuovi mezzi di ricerca della prova digitali nell'ambito dell'indagine penale. Dopo una prima *pars destruens*, in cui vengono evidenziate le principali inadeguatezze dell'attuale assetto normativo ed interpretativo, l'autore prosegue attraverso un approccio maggiormente propositivo, tentando di delineare gli attributi comuni ad una categoria di operazioni particolarmente invasive, come tali meritevoli di essere destinatarie di alcune previsioni di garanzia in prospettiva *de iure condendo*.

La individualización de las posiciones de garantía en el sector de la tutela de los datos personales constituye un tema casi inexplorado, tanto por la doctrina como por la jurisprudencia. No obstante, la entrada en vigencia del Reglamento Europeo de Protección de Datos Personales y del correspondiente decreto de adecuación (Decreto Legislativo 101/2018) justifican una mayor atención a esta materia. El presente artículo tiene por objeto analizar la reconstrucción de las posiciones de garantía en el sector de la tutela de los datos y el consecuente encuadramiento de las relaciones intersubjetivas entre las garantías.

This paper focuses on new IT evidence research tools in criminal investigations. After a first *pars destruens*, where the main inconsistencies of the current regulatory and scholarly framework are highlighted, the Author offers a more constructive approach, trying to outline the common features of very intrusive activities, as such deserving to be surrounded by several safeguards from a *de iure condendo* standpoint.

Sommario

1. Considerazioni introduttive.

La «metamorfosi investigativa» conseguente alla diffusione delle nuove tecnologie rappresenta un dato riconosciuto tra gli studiosi del processo penale[1].

Si è al cospetto di un fenomeno particolarmente insidioso, non soltanto per l'attitudine delle nuove metodiche di accertamento ad incidere diverse delle libertà fondamentali sancite a livello costituzionale e sovranazionale, ma anche perché la tendenza in esame risulta sovente giustificata in forza di suggestive esigenze di tutela della collettività, capaci di ammantare di aprioristica legittimità il sacrificio imposto alle prerogative dei singoli.

Eppure, come bene è stato evidenziato, la salvaguardia della sicurezza pubblica - e dunque anche le attività di accertamento giustificate da necessità di prevenzione e repressione degli illeciti penali – conservano un senso solo in quanto non finiscano per comprimere in maniera sproporzionata quegli stessi valori che mirano in definitiva a preservare. Diversamente, si giungerebbe infatti al paradosso per cui le libertà dell'individuo - ove non aggredite dai fenomeni criminosi oggetto di contrasto - verrebbero comunque annichilite dalla minaccia di un'ingerenza ubiquitaria dell'autorità nell'esistenza di ciascun consociato[2].

La necessità di un adeguato bilanciamento tra le esigenze in conflitto e le inedite caratteristiche delle indagini digitali obbligano dunque ad un ripensamento di molti dei tradizionali paradigmi giuridici come sino ad oggi conosciuti, costringendo ad un inedito sforzo ricostruttivo l'interprete che si voglia misurare con il tema.

La riflessione appare ben avviata in tal senso sul piano dell'indagine costituzionale. Alla diffusione di nuovi ed invasivi strumenti di indagine si accompagna infatti il dibattito relativo ai c.d. "nuovi diritti", diretto ad isolare nuove situazioni giuridiche attive idonee a soddisfare le esigenze di tutela proprie del mutato contesto socio-tecnologico, principalmente sulla scia di alcune importanti affermazioni rese sul punto dalla giurisprudenza costituzionale tedesca[3].

L'elaborazione non sembra però altrettanto matura all'interno della legislazione ordinaria, ed in particolare nell'ambito della disciplina processuale penale, sistema cui sarebbe in verità assegnato in via principale il compito di regolamentare le attività in questione, offrendo concreta protezione ai diritti consacrati nella Carta Fondamentale[4], ma che appare affetto da un preoccupante immobilismo.

2. Stato dell'arte della normativa processuale penale.

La principale base giuridica utilizzata per giustificare il ricorso agli strumenti di indagine in questione continua infatti ad essere rappresentata dalla disciplina offerta agli artt. 266 ss. c.p.p. in materia di intercettazioni di comunicazioni e conversazioni. L'istituto, almeno secondo la configurazione offertane dalla giurisprudenza di legittimità, mediante un'artificiosa e discutibile scomposizione postuma dell'atto investigativo, finisce così per assumere il ruolo di versatile *passe-partout* capace di giustificare il compimento di attività anche solo parzialmente

[1] Signorato (2018), p. 1 ss, cui si deve anche l'efficace espressione citata nel testo; nonché almeno Di Paolo (2008), *passim*; Marinelli (2007a), *passim*.

[2] Si vedano al riguardo le puntuali considerazioni espresse in più occasioni dalla Corte eur. dir. uomo, secondo cui «*a system of secret surveillance set up to protect national security may undermine or even destroy democracyunder the cloak of defending it*». Così, da ultimo, Corte eur. dir. uomo, I sez., *Big Brother watch and others c. Regno Unito*, 13 settembre 2018, par. 308.

[3] Si allude *in primis* a BVerfGE, 1 BvR 209, 269, 362, 420, 440, 484, 15 dicembre 1983, in materia di "diritto all'autodeterminazione informativa", cui è poi seguita BVerGE, 120, 274, 27 febbraio 2008, annotata da Flor (2009), specificamente relativa al contesto di misure investigative penali e "diritto alla riservatezza ed integrità dei sistemi informatici". La dottrina costituzionale italiana è divisa in ordine alla possibilità di una tale operazione "creativa". Favorevole Barbera (1975), p. 91; Più scettico invece Pace (2003), p. 4 ss. Cfr. anche Modugno (1995), *passim*.

[4] Funzione riassunta nella celebre definizione di matrice tedesca della procedura penale quale «diritto costituzionale applicato». Cfr. al riguardo Illuminati (2008), p. 521 ss.; nonché Negri (2011), p. 13 ss., anche per ulteriori riferimenti bibliografici.

dirette all'acquisizione di contributi comunicativi *ex* art. 15 Cost.

Ciò emerge con chiarezza all'interno del tessuto argomentativo del noto ed ormai risalente *leading-case* in materia di c.d. videoriprese investigative, integranti attività di intercettazione nel momento in cui documentino comportamenti di tipo comunicativo, e qualificabili invece alla stregua di c.d. prove atipiche limitatamente alla registrazione di frammenti di vita di diversa natura[5].

Detta registrazione diviene però una "prova incostituzionale", come tale inutilizzabile, nel momento in cui ha ad oggetto condotte non comunicative filmate all'interno del domicilio. Come noto, la riserva di legge di cui all'art. 14 Cost. vieta infatti l'intrusione in assenza di un'apposita base legale, ma la "video-intercettazione" domiciliare, di contro, rimane ammissibile al ricorrere del presupposto di cui all'art. 266, comma 2, c.p.p.[6].

Si tralascia però così di considerare che il peculiare mezzo impiegato per la captazione comunicativa implica pressoché inevitabilmente la contestuale apprensione di contributi di diversa natura, con l'effetto di legittimare comunque un'invasione *contra legem* dello spazio domiciliare, a prescindere dal problema concettualmente diverso inerente alla spendita processuale delle risultanze del c.d. *homewatching*. Come ricordato, nessuna norma consente infatti di introdursi nell'abitazione per fini ulteriori rispetto all'intercettazione di comunicazioni tra presenti.

Una struttura argomentativa pressoché analoga continua a caratterizzare le più recenti decisioni relative all'impiego del c.d. captatore informatico. Anche in questo caso infatti, il ricorso allo strumento è stato considerato legittimo in forza delle previsioni di cui agli artt. 266 ss. c.p.p. per procedere all'intercettazione, limitatamente ai procedimenti per "criminalità organizzata"[7], quantunque esso permetta di documentare un'amplissima mole di informazioni anche diverse da quelle riconducibili al *genus* comunicativo. In quest'ultimo caso le perplessità derivanti dalla ricostruzione prescelta sono ulteriormente aggravate dalla ragguardevole potenza intrusiva del mezzo, che non si limita a consentire la registrazione visiva di mere condotte, come avviene nel caso delle videoriprese, ma si estende sino a rendere possibile una sorveglianza in tempo reale dell'attività dell'utente nonché l'accesso alla memoria del dispositivo infettato[8].

Viene poi appunto in rilievo la discutibile categoria residuale dei c.d. atti investigativi atipici, insieme che ricomprende al suo interno tutte le acquisizioni insuscettibili di essere qualificate alla stregua di attività di intercettazione[9].

In questo caso, l'assenza di un'adeguata tipizzazione normativa è ancora più evidente: non sono infatti in alcuna maniera specificati presupposti, modalità esecutive e limiti di utilizzo delle risultanze di operazioni capaci di pregiudicare le aspettative di riservatezza dei singoli. Per quanto attraverso il compimento di dette attività non sia infatti possibile realizzare acquisizioni che importino un sacrificio per le libertà fondamentali espressamente riconosciute in Costituzione[10], risulta d'altro canto pacifica la deroga al diritto al rispetto della vita privata sancito dall'art. 8 C.E.D.U. conseguente all'utilizzo di molte delle tecniche in discussione[11]. È quasi scontato denunciare allora il contrasto di tale assetto con la fonte da ultimo richiamata in forza del mancato rispetto della riserva di legge prescritta dalla norma sovranazionale.

In una singolare eterogenesi dei fini, le norme processuali - lungi dal circoscrivere i poteri dell'inquirente – finiscono paradossalmente per assolvere all'antitetica funzione di lasciapas-

[5] Cass. Sez. Un., 28 marzo 2006, n. 26795, annotata da Camon (2006), p. 1550.

[6] Diffusamente sul tema, tra gli altri, ed in aggiunta al contributo citato alla nota immediatamente precedente, Triggiani (2014), p. 151 ss.

[7] Cass. Sez. Un., 28 aprile 2016, n. 26889, in *Cass. pen.*, 2016, p. 3546, con nota di Nocerino (2016), nonché annotata da Lasagni (2016); Cajani (2016). Secondo il *dictum* in esame infatti, la previsione speciale di cui all'art. 13 del d.l. n. 152/1991, che permette l'intercettazione domiciliare anche in assenza di fondati motivi per ritenere che là si stia svolgendo l'attività criminosa, consentirebbe di prescindere dall'indicazione del contesto spaziale di esecuzione dell'intercettazione al momento della sua autorizzazione, rendendo conseguentemente possibile l'attivazione dell'intercettazione itinerante.

[8] Per una rassegna degli usi dello strumento, Brighi (2018), p. 221 ss.; Camon (2017a), p. 91.

[9] Critico al riguardo Camon (2017b), p. 96 ss. Appare in effetti lecito domandarsi se il riconoscimento all'inquirente di poteri innominati privi di specifica disciplina legale risponda in maniera idonea all'esigenza di governare adeguatamente lo svolgimento delle indagini alla luce della moltitudine di tecniche investigative oggigiorno disponibili. Si veda anche, tra gli altri, Parlato (2018), p. 292 ss.

[10] Questo è infatti il limite negativo unanimemente attribuito all'insieme di attività in esame che, appunto in quanto sguarnite di espressa disciplina legale, risultano inidonee a soddisfare la riserva di legge imposta dalle previsioni di rango fondamentale. Si veda, per tutti, Conti (2007), p. 162.

[11] Basti pensare alla localizzazione satellitare mediante sistema G.P.S., qualificata appunto quale attività di indagine atipica dagli interpreti nazionali, ma integrante un'ingerenza nel diritto al rispetto della vita privata *ex* art. 8 C.E.D.U. secondo i giudici di Strasburgo. A tale ultimo proposito si veda Corte eur. dir. uomo, V sez., *Uzun c. Germania*, 2 settembre 2010; nonché, più di recente, Corte eur. dir. uomo, V sez., *Ben Faiza c. Francia*, 8 febbraio 2018. In dottrina cfr. Iovene (2012), p. 3556 ss.; nonché Bene (2014), p. 366.

sare utile a giustificare le più diverse intrusioni all'interno della sfera di intimità. Ad uscire mortificata dal quadro sinteticamente tracciato è la stessa essenza garantista delle regole del rito, mistificate nel loro significato più profondo ed impropriamente ricondotte al ruolo di «arnese poliziesco»[12] funzionale a consentire le più diverse ingerenze.

3. Per un approccio alternativo al problema del controllo digitale: prospettive *de iure condendo*.

A fronte di una situazione così compromessa, è difficilmente revocabile in dubbio che una possibile soluzione debba necessariamente passare attraverso un organico intervento normativo che si preoccupi di regolamentare in maniera adeguata il ricorso alle nuove tecniche investigative.

Del resto, questa è stata la strada seguita da alcuni dei più importanti ordinamenti europei. Si pensi alla realtà francese, in cui – nel campo delle misure di contrasto alla criminalità organizzata – sono oggi specificamente disciplinate l'intercettazione di corrispondenza elettronica e l'identificazione dei dati tecnici di connessione (artt. 706-95-1 ss. del codice di rito), le intercettazioni "ambientali" sonore e visive (artt. 706-96-1 ss.) e la captazione occulta da remoto di dati informatici (artt. 706-102-1 ss.). Rilevano inoltre l'esempio di Spagna e Germania, che hanno entrambe inteso regolamentare il ricorso ai mezzi di ricerca della prova digitali mediante l'adozione di due appositi provvedimenti normativi, rispettivamente nel 2015[13] e nel 2017[14].

Ben più timido è l'approccio del nostro legislatore che, palesando una certa affinità concettuale alla ricordata impostazione atomistica sino ad ora prediletta dalla giurisprudenza di legittimità, si è limitato a prevedere all'art. 266, commi 2 e 2 *bis*, c.p.p. la facoltà di utilizzo del c.d. captatore informatico esclusivamente quale mezzo per l'intercettazione di conversazioni tra presenti. È evidente come in tale maniera si trascurino però gli ulteriori utilizzi del polivalente strumento, quali le c.d. perquisizioni *on-line* ed il monitoraggio in tempo reale dell'attività dell'utente, che continueranno così ad essere attratti nell'area dell'atipicità[15].

A ben vedere, il difetto appena denunciato non si limita a testimoniare la pur preoccupante approssimazione che caratterizza il recente intervento normativo. Esso induce infatti più in generale a riflettere sull'effettiva praticabilità di una regolamentazione che si risolva in un'analitica codificazione dei singoli mezzi di ricerca della prova, secondo l'esempio fornito dagli ordinamenti stranieri poco sopra menzionati. È infatti verosimile che una tale strategia finirebbe per tralasciare alcune delle numerose potenzialità applicative offerte dalle nuove tecnologie, obbligando peraltro ad una costante opera di aggiornamento a seguito della presumibile diffusione di sempre nuovi ritrovati.

Si potrebbe allora pensare di preferire una diversa impostazione, che si caratterizzi per l'esistenza di una disciplina generalmente applicabile alle attività insuscettibili di essere ricondotte ad una fattispecie tipica esistente, scongiurando così il ricorso alla categoria totalmente deformalizzata dell'atto investigativo atipico.

L'idea non è del tutto nuova, ma risulta al contrario già avanzata nel momento in cui è stata suggerita la possibilità di immaginare una nuova norma, un «ipotetico "art. 189 bis"» che potesse sostituire alla libertà delle forme ancora oggi invalsa la necessità di rispettare alcuni requisiti minimi di garanzia per il ricorso ai più invasivi mezzi di ricerca della prova tecnologicamente assistiti[16].

[12] Negri (2016), p. 44 ss.
[13] *Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.*
[14] *Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17/8/2017.*
[15] Lo segnalano, tra gli altri, Mancuso (2018), p. 194. Più in generale sul tema cfr. anche Rivello (2018), p. 101 ss.
[16] In questi termini Camon (2014), p. 217. In senso analogo Marcolini (2015), p. 789-790, il quale caldeggia l'introduzione di specifiche previsioni dedicate all'«atto investigativo atipico», concetto connotato da un finalismo «investigativo-probatorio» dell'attività e dall'idoneità della stessa ad incidere un diritto fondamentale.

4. I confini della categoria.

Occorrerebbe però delineare in maniera più specifica l'oggetto di una simile previsione, non foss'altro che per garantire l'osservanza della riserva di legge prescritta in materia[17].

A tal fine sembra conveniente procedere per approssimazione "in negativo", prendendo le mosse dall'esame di alcuni criteri classificatori tutt'ora diffusi, che appaiono tuttavia da scartare in quanto incapaci di assolvere adeguatamente alla loro funzione.

Avrebbe innanzitutto poco senso assumere come riferimento un criterio eminentemente spaziale, inteso ad imporre l'applicazione di determinate tutele solo sulla base del luogo di esecuzione dell'atto.

Le tecnologie attualmente disponibili svincolano infatti le operazioni in esame da un preciso ambito di riferimento "geografico" determinabile *ex ante*, consentendo ricerche itineranti e potenzialmente ubiquitarie[18].

Sarebbe inoltre inattuale valorizzare la tipologia pubblica o privata dell'ambito spaziale di acquisizione del dato. Il tradizionale assioma per cui ogni condotta avvenuta in luogo pubblico o esposto al pubblico sarebbe in quanto tale estranea a qualsiasi ragionevole pretesa di intimità poiché liberamente osservabile da chicchessia, e dunque documentabile senza il necessario rispetto di formalità di sorta[19], si espone infatti a diverse considerazioni critiche.

Rilevano in tal senso le potenzialità dei mezzi attualmente disponibili, capaci di assicurare la conoscenza di informazioni precluse alla vista dell'osservatore comune, inficiando dunque la validità della deduzione appena ricordata[20]. A ciò deve poi aggiungersi che, anche in contesti non rigorosamente privati, è senz'altro possibile ammettere l'esistenza di comportamenti comunque assistiti da una qualche aspettativa di riservatezza. Proprio per tali ragioni, specie nell'ambito di realtà ordinamentali diverse da quella italiana, si teorizza già l'esistenza di una sorta di "diritto all'anonimato in contesti pubblici", che imporrebbe dunque l'attuazione di limitazioni legali anche per la documentazione di condotte che hanno luogo in contesti pubblici o semi-pubblici[21].

Sembra parimenti da rifuggire un approccio c.d. "*content-based*", teso a circoscrivere il novero delle operazioni meritevoli di protezione in ragione della natura delle informazioni oggetto di acquisizione[22].

Analogamente a quanto si è già osservato in relazione al parametro spaziale, anche tale soluzione sembra di difficile praticabilità alla luce delle caratteristiche degli strumenti attualmente impiegati, che non consentono di prevedere anticipatamente la tipologia e la "sensibilità" dell'oggetto di documentazione.

Su di un piano più concettuale, si rischierebbe poi di riconoscere eccessiva consistenza ad un principio di c.d. «neutralità tecnica», il quale giustificherebbe a sua volta il ricorso ad una disciplina uniforme per tutte le acquisizioni di un insieme di dati riconducibili ad un medesimo *genus*, predicando appunto l'indifferenza delle modalità tecniche concretamente utilizzate per la raccolta ai fini dell'individuazione della disciplina applicabile[23].

Tale costruzione rischia però di condurre ad esiti irragionevoli. Ferma restando la superfluità di un'analitica tipizzazione delle modalità tecniche di apprensione ai fini del rispetto della riserva di legge[24], non è possibile disconoscere che il mezzo materialmente impiegato per l'acquisizione non può per definizione essere considerato neutro rispetto ai risultati dell'acquisizione stessa. Al contrario, tale variabile possiede una precisa influenza sull'ampiezza delle informazioni suscettibili di essere documentate e dunque, in definitiva, sulla stessa invasività della misura.

[17] Rileva ancora il disposto dell'art. 8, par. 2, della Convenzione e.d.u., nonché sicuramente il combinato disposto degli artt. 7, 8 e 52 della Carta dei Diritti Fondamentali dell'Unione Europea.

[18] La caratteristica in esame è ben evidenziata da Gaito, Fùrfaro (2016), p. 309 ss., e da Filippi (2016), p. 348, con specifico riguardo allo strumento del captatore informatico.

[19] Sul filone giurisprudenziale in questione si veda Marinelli (2007b), p. 4643 ss.

[20] Basti limitarsi al confronto tra attività di pedinamento "tradizionali" ed utilizzo di sistema di localizzazione G.P.S.: «tra le due categorie passa una differenza di tale ampiezza, da non poter essere ignorata». In questi termini Camon (2005), p. 634.

[21] Se ne dà atto in Di Paolo (2009), p. 225 ss.

[22] Approccio che, in forza di quanto si è detto *supra*, appare tuttavia dominante all'interno della nostra giurisprudenza di legittimità, innanzitutto impegnata a vagliare l'eventuale natura comunicativa delle informazioni captate al fine di qualificare l'attività acquisitiva alla stregua di un'intercettazione.

[23] Sul tema, sebbene limitatamente al valore neutrale della tecnologia ai fini del rispetto della riserva di legge, Lasagni (2016), p. 11.

[24] Questa appunto la tesi dell'autrice citata alla nota precedente.

Così, esemplificando, la video-intercettazione è in grado di assicurare la conoscenza di un patrimonio informativo indubbiamente più esteso rispetto a quello derivante da una captazione posta in essere mediante il ricorso a strumenti di semplice fonoregistrazione, essendo se non altro in grado di carpire una serie di condotte comunicative non verbali che sfuggirebbero invece all'intercettazione "tradizionale". In maniera analoga, il captatore informatico – consentendo l'accesso diretto al dispositivo infettato dalla prospettiva del suo utilizzatore - è in grado di assicurare l'acquisizione intellegibile degli scambi di corrispondenza coperti da cifratura c.d. *pin to pin*, che non sarebbe invece possibile ottenere mediante la classica intercettazione *in itinere* del flusso comunicativo telematico senza la collaborazione del detentore della chiave di cifratura dei messaggi[25].

Una categorizzazione che assuma come riferimento la tipologia dell'oggetto di acquisizione rischierebbe allora di non tenere adeguatamente conto di tali importanti distinzioni, legittimando un trattamento normativo omogeneo.

Ciò risulterebbe tuttavia difficilmente conciliabile con la corretta applicazione del fondamentale principio di proporzionalità, secondo il quale ad attività capaci di di incidere più profondamente il diritto alla riservatezza deve essere riservata una disciplina legale più rigorosa rispetto a quella propria di operazioni meno intrusive[26].

5. Il controllo occulto e continuativo come categoria probatoria.

Un approccio maggiormente adeguato all'esigenza segnalata in apertura del precedente paragrafo sembra allora quello teso a valorizzare le caratteristiche della stessa attività acquisitiva.

In quest'ottica si rivela assai prezioso il ricorso alla categoria del controllo occulto e continuativo. Proprio questa endiadi sembra infatti in grado di sintetizzare efficacemente i connotati di maggiore afflittività dell'atto.

Quanto al primo dei due attributi, già in epoca alquanto risalente la giurisprudenza della Corte e.d.u. ha dimostrato una precisa consapevolezza in tal senso, evidenziando la speciale invasività di operazioni clandestine volte a carpire informazioni di natura riservata, relegando tale eventualità ad ipotesi assolutamente eccezionale, legittimata solamente «a malincuore» in ragione di esigenze di contrasto alle forme più gravi di criminalità[27].

Del resto, la natura occulta della misura neutralizza ogni possibilità di autocensurarsi da parte del destinatario passivo, che potrebbe «abbandonarsi a comportamenti molto privati e imbarazzanti» senza la possibilità di orientare in maniera più consapevole la propria condotta[28].

Su di un piano più eminentemente processuale, la sorveglianza clandestina lo pone altresì in una posizione di consistente svantaggio, posto che egli, una volta terminate le operazioni, sarà sovente costretto ad una defatigante e talvolta infruttuosa retrospettiva diretta a circostanziare il significato delle emergenze raccolte a suo carico, peraltro con il rischio di non essere sempre in grado di vagliare l'effettiva completezza dell'attività esperita. In assenza di adeguate garanzie, è reale infatti il rischio che informazioni eventualmente utili alla sua difesa siano pretermesse anche solo perché considerate *prima facie* irrilevanti rispetto all'oggetto dell'accertamento[29].

I rimedi garantiti al soggetto passivo dell'operazione acquisitiva risultano poi giocoforza posticipati ad un momento successivo al termine delle operazioni, quando la lesione alle aspettative di intimità si è già integralmente prodotta.

Venendo alla seconda caratteristica, la natura continuativa del controllo vale poi a connotare ulteriormente in termini di speciale invasività le attività in esame.

L'attributo implica innanzitutto un'acquisizione effettuata in tempo reale[30], che cagiona

[25] Cfr. Di Stefano, Fiammella (2018), p. 122 ss.
[26] Più diffusamente al riguardo, volendo, Nicolicchia (2017), p. 3 ss.
[27] Corte eur. dir. uomo, *Klass and others c. Germania*, 6 settembre 1978, par. 68.
[28] Camon (1999), p. 1193.
[29] Un esempio lampante in tal senso è offerto dalle norme recentemente introdotte dal d.lgs. n. 216/2017 relativamente alla procedura di selezione e stralcio delle intercettazioni basata su di un generico parametro di "rilevanza". Diffusamente al riguardo, Morelli (2018), p. 109 ss.
[30] Solo in tal caso assume infatti significativo la natura continuativa dell'operazione; se si trattasse di procurarsi infatti un dato già precostituito, essa non potrebbe che risolversi in un'operazione istantanea, che si esaurisce nel momento stesso dell'acquisizione.

l'immediata fuoriuscita del dato appreso dalla sfera di controllo del titolare, massimizzando così il rischio di una sua diffusione prima ancora che egli abbia modo di porre in essere ogni iniziativa volta a contenerne la circolazione.

Rileva però soprattutto la dimensione riferita all'estensione diacronica del controllo, anch'essa compresa nel riferimento alla sua natura continuativa.

Come è stato efficacemente sottolineato, «differenze di quantità finiscono dunque per tradursi in differenze di qualità», ed anche la documentazione di condotte non strettamente riservate, se prolungata nel tempo, può arrivare ad integrare una consistente lesione alle aspettative di riserbo[31].

Non a caso, la durata della sorveglianza è espressamente menzionata dai giudici di Strasburgo tra gli indici idonei a qualificare l'intensità della lesione arrecata al diritto al rispetto della vita privata[32].

Queste considerazioni rappresentano un semplice prodromo rispetto ad una riflessione più approfondita, tesa innanzitutto a delineare in maniera più analitica il perimetro della categoria evocata e – successivamente – ad individuare nel dettaglio i connotati delle garanzie da assicurare in occasione del compimento delle attività sussumibili all'interno del *genus*.

Per quanto provvisorie, esse sembrano però sufficienti a testimoniare un significativo disagio nel constatare come la crescita esponenziale delle occasioni di aggressione alla sfera intima dell'individuo resa possibile dal progresso tecnologico mal si concili con il quadro normativo vigente, espressione di un bilanciamento tra esigenze cognitive dell'indagine e libertà fondamentali che appare oggi insoddisfacente, e che occorre pertanto ripensare a partire dalle sue stesse premesse sistematiche.

Bibliografia

Barbera, Augusto (1975): *Commento all'art.2*, in Branca, Giuseppe (editor): *Commentario della Costituzione italiana. Art. 1-12. Principi fondamentali* (Bologna, Zanichelli)

Bene, Teresa (2014): "Il pedinamento elettronico: truismi e problemi spinosi", in scalfati, Adolfo (editor): *Le indagini atipiche* (Torino, Giappichelli), pp. 347-359

Brighi, Raffaella (2018): "Funzionamento e potenzialità investigative del *malware*", in Giostra, Glauco, Orlandi, Renzo (editors): *Nuove norme sulle intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche* (Torino, Giappichelli), pp. 211-234

Cajani, Francesco (2016): "Odissea del captatore informatico", *Cassazione penale*, pp. 4139-4151

Camon, Alberto (1999): "Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali", *Cassazione penale*, pp. 1192-1213

Camon, Alberto (2005): "L'acquisizione dei dati sul traffico delle comunicazioni", *Rivista italiana di diritto e procedura penale*, pp. 594-650

Camon, Alberto (2006): "Le Sezioni Unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni nuovi dubbi", *Rivista italiana di diritto e procedura penale*, pp. 1550-1569

[31] Camon (2014), p. 215.

[32] «*This assessment depends on all the circumstances of the case, such as the nature, scope and* duration *of the possible measures*», secondo la ormai risalente ma ancora attuale pronuncia Corte eur. dir. uomo, *Klass and others c. Germania*, cit., par. 50.

Camon, Alberto (2014): "Innovazioni tecnologiche e mezzi di ricerca della prova", in Andretta, Massimo, Fondaroli, Desirée, Gruppioni Giorigio (editors): *Dai "casi freddi" ai "casi caldi". Le indagini storiche e forensi fra saperi giuridici e investigazioni scientifiche* (Padova, Cedam), pp. 209-217

Camon, Alberto (2017a): "Cavalli di Troia in Cassazione", *Archivio della nuova procedura penale*, pp. 91-100

Camon, Alberto (2017b): "La fase che "non conta e non pesa": indagini governate dalla legge?", in *Legge e potere nel processo penale. Atti del Convegno, Bologna 4 e 5 novembre 2016* (Padova, Cedam) pp. 93-114

Conti, Carlotta (2007): *Accertamento del fatto e inutilizzabilità nel processo penale* (Padova, Cedam)

Di Paolo, Gabriella (2008): "*Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione* (Padova, Cedam)

Di Paolo, Gabriella (2009): "Acquisizione dinamica dei dati relativi all'ubicazione del cellulare ed altre forme di localizzazione tecnologicamente assistita. Riflessioni a margine dell'esperienza statunitense", in *Le intercettazioni di conversazioni e comunicazioni. Un problema cruciale per la civiltà e l'efficienza del processo e per le garanzie dei diritti* (Milano, Giuffrè), pp. 221-239

Di Stefano, Michelangelo, Fiammella Bruno (2018): *Intercettazioni: remotizzazione e diritto di difesa nell'attività investigativa (profili d'intelligence*), II edizione, (Milano, Wolters Kluwer)

Filippi, Leonardo (2016): "L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico)", *Archivio penale*, pp. 348-353

Flor, Roberto (2009): "Brevi riflessioni a margine della sentenza del *Bundesverfassungsgericht* sulla c.d. *Online Durchsuchung*", *Rivista trimestrale di diritto penale dell'economia*, pp. 695-716

Gaito, Alfredo e Fùrfaro, Sandro (2016): "Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività", *Archivio penale*, pp. 309-330

Illuminati, Giulio (2008): "Costituzione e processo penale", *Giurisprudenza italiana*, pp. 521-528

Iovene, Federica (2012): "Pedinamento satellitare e diritti fondamentali della persona", *Cassazione penale*, pp. 3556-3565

Lasagni, Giulia (2016): "L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"", *www.penalecontemporaneo.it*

Mancuso, Enrico Maria (2018): "Le acquisizioni mediante captatore non disciplinate dalla legge", in Giarda Angelo, Giunta, Fausto, Varraso Gianluca (editors): *Dai decreti attuativi della legge "Orlando" alle novelle di fine legislatura* (Padova, Cedam), pp. 193-216

Marcolini, Stefano (2015): "Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta", *Cassazione penale*, pp. 760-792

Marinelli, Claudio (2007a): *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, (Torino, Giappichelli)

Marinelli, Claudio (2007b): "Le videoriprese investigative in luoghi esposti al pubblico: verso la progressiva emersione dei criteri di qualificazione degli ambiti spaziali soggetti alle operazioni", *Cassazione penale*, pp. 4643-4651

Modugno, Franco (1995): *I nuovi diritti nella giurisprudenza costituzionale* (Torino, Giappichelli)

Morelli, Francesco (2018): "Il nuovo volto delle intercettazioni: procedimento selettivo e riservatezza dei dialoghi intercettati" in Giarda Angelo, Giunta, Fausto, Varraso Gianluca (editors): *Dai decreti attuativi della legge "Orlando" alle novelle di fine legislatura* (Padova, Cedam), pp. 105-138

Negri, Daniele (2011): "Agli albori di un paradigma dell'Italia repubblicana: il processo penale come "diritto costituzionale applicato", in negri, Daniele, Pifferi, Michele (editors): *Diritti individuali e processo penale nell'Italia repubblicana. Materiali dall'incontro di studio. Ferrara, 12-13 novembre 2010* (Milano, Giuffrè)

Negri, Daniele (2016): "La regressione della procedura penale ad arnese poliziesco", *Archivio penale*, pp. 44-54

Nicolicchia, Fabio (2017): "I limiti fissati dalla Corte costituzionale tedesca agli strumenti di controllo tecnologico occulto: spunti per una trasposizione nell'ordinamento italiano", *Archivio penale* (rivista web), pp. 1-14

Nocerino, Wanda (2016): "Le sezioni unite risolvono l'enigma: l'utilizzabilità del "captatore informatico" nel processo penale", *Cassazione penale*, pp. 3565-3584

Pace, Alessandro (2003): *Problematica delle libertà costituzionali. Parte generale: introduzione allo studio dei diritti costituzionali* (Padova, Cedam)

Parlato, Lucia (2018): "Problemi insoluti: le perquisizioni *on-line*", in Giostra, Glauco, Orlandi, Renzo (editors): *Nuove norme sulle intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche* (Torino, Giappichelli), pp. 289-323

Rivello, Pier Paolo (2018): "Le intercettazioni mediante captatore informatico", in Mazza, Oliviero (editor): *Le nuove intercettazioni* (Torino, Giappichelli), pp. 101-138

Signorato, Silvia (2018): *Le indagini digitali; profili strutturali di una metamorfosi investigativa* (Torino, Giappichelli)

Triggiani, Nicola (2014): "Le videoriprese investigative", in scalfati, Adolfo (editor): *Le indagini atipiche* (Torino, Giappichelli), pp. 141-166

L'accesso transfrontaliero all'*electronic evidence*, tra esigenze di effettività e tutela dei diritti

El acceso transfronterizo a evidencia electrónica, entre exigencias de efectividad y tutela de derechos

Transnational Access to Electronic Evidence Between Effectiveness and the Need to Protect Rights

Veronica Tondi
Dottoranda di ricerca presso la LUISS Guido Carli
vtondi@luiss.it

Diritti fondamentali, Intercettazioni | Derechos fundamentales, Interceptación de comunicaciones | Fundamental rights, Intrusive surveillance

Abstracts

Il contributo si propone di prendere in esame i profili più significativi legati all'accesso transfrontaliero alla prova digitale, di crescente rilevanza in considerazione delle odierne tensioni tra limitazione della giurisdizione statale entro i confini nazionali e dematerializzazione dei dati informatici, non agevolmente collocabili in un determinato ambito territoriale. Oggetto di trattazione sono specificamente le recenti proposte di Regolamento e di Direttiva dell'Unione europea in materia di ordini europei di produzione e di conservazione dell'*electronic evidence*, considerati anche nel loro inquadramento nell'ambito del sistema normativo vigente, con particolare riguardo alle previsioni in materia di ordine europeo di indagine. Ad una sintetica analisi delle principali questioni relative ai rapporti tra l'Unione europea e Stati terzi in materia di accesso alla prova digitale seguono quindi alcune considerazioni conclusive sul nuovo modello di cooperazione fondato sul contatto diretto con il privato prestatore di servizi non sottoposto alla giurisdizione dello Stato procedente, in assenza, in linea di principio, di intermediazioni.

El presente trabajo tiene por objeto examinar las principales cuestiones relacionadas con el acceso transfronterizo a evidencia electrónica, tema de creciente relevancia en consideración a la problemática interacción entre la limitación de la jurisdicción estatal y la desmaterialización de los datos informáticos. El articulo aborda principalmente las recientes propuestas de reglamento y directiva de la Unión Europea en materia de ordenes europeas de producción y conservación de evidencia electrónica. A continuación, se analizan algunos de los principales problemas relativos a la relación entre la Unión Europea y terceros estados en asuntos de acceso transfronterizo a evidencia electrónica. Posteriormente, se efectúan algunas consideraciones finales sobre el nuevo modelo de cooperación directa con los proveedores de servicios de internet establecidos fuera de la jurisdicción estatal.

This paper aims to examine the most important issues involved by transnational access to electronic evidence. The latter is increasingly important due to the problematic interaction between the limitation of State jurisdiction within national boundaries and the dematerialization of data usable as evidence in criminal proceedings. The work mainly deals with the recent proposals of EU Regulation and Directive on European Production and Conservation Orders, aiming to analyse also their interference with the current law on judicial cooperation in criminal matters, especially with regard to the European Investigative Order. Some of the main problems concerning the relationship between the European Union and third States concerning transnational access to electronic evidence,

are then briefly examined, and followed by some final remarks on the new model of direct cooperation with service providers established outside the State jurisdiction.

Sommario

1. Premessa.

Lo stretto intreccio tra nuove tecnologie e fenomeni criminali, l'esigenza di rendere i dispositivi e i sistemi informatici oggetto delle attività di indagine e istruttorie volte all'acquisizione di elementi di prova, e la necessità di avvalersi delle opportunità offerte dal progresso tecnico per le finalità della giustizia penale[1], appaiono ormai acquisizioni incontestabili.

Tali sistemi costituiscono invero, in misura crescente, tanto gli strumenti impiegati per la commissione di reati, quanto, e conseguentemente, la sede di conservazione di rilevanti dati e informazioni suscettibili di assumere valenza probatoria.

Il carattere immateriale dei dati, la loro agevole trasferibilità da un *server* a un altro, la mobilità degli strumenti utilizzati per la loro conservazione, così come l'utilizzo di tecnologie quali il *cloud computing*, idonei a comportare la scissione delle risorse da un supporto fisico e la loro diffusione in diversi sistemi e Paesi, non sempre agevolmente individuabili, oltre che la possibilità di una loro gestione ad opera di differenti *providers*[2], pongono problemi nuovi e particolarmente significativi nello svolgimento delle attività di indagine, di ricerca e di assunzione della prova, e sovente l'esigenza di un accesso alla cd. *electronic evidence* a carattere transfrontaliero.

In proposito, le questioni legate all'accesso a quest'ultima appaiono inserite nel più ampio problema dell'acquisizione della prova all'estero, alla luce del fatto che, mentre tanto le attività economiche, quanto quelle criminose eccedono in misura crescente i confini nazionali, significative differenze tra le normative nazionali in materia di assunzione e utilizzabilità della prova, sono frequentemente di ostacolo all'utilizzo della stessa quando essa sia assunta all'estero, secondo regole diverse da quelle dell'ordinamento di riferimento.

In tale ambito, tradizionalmente regolato da trattati internazionali, si sono inseriti significativi interventi normativi dell'Unione europea, tesi ad agevolare la circolazione della prova nello spazio giudiziario europeo e a rendere più agevole la cooperazione internazionale, secondo modalità tali da superare il modello della rogatoria, caratterizzato dall'intervento di autorità "centrali", a carattere amministrativo, sebbene l'intervento del ministro della giustizia sia stato già fortemente ridimensionato dalla Convenzione di assistenza giudiziaria del 2000. Si pone poi la questione della preferibilità di un approccio che sia tale da realizzare il mutuo riconoscimento dei provvedimenti adottati dagli Stati membri, o di un'impostazione che invece valorizzi l'armonizzazione delle disposizioni normative nazionali.

Gli strumenti previsti dal diritto vigente, disciplinati dal diritto dell'Unione europea e recepiti nell'ordinamento interno, che vanno nella direzione dell'incremento dell'efficienza e della rapidità della cooperazione tra Stati membri in materia di ricerca e acquisizione della prova sono rappresentati dalle squadre investigative comuni - regolate dalla Convenzione di Bruxelles in materia di assistenza giudiziaria del 2000 e dalla decisione quadro 2002/465/GAI, a cui è stata data attuazione in Italia solo con il d. lgs. 34/2016 - e dall'ordine europeo di indagine penale, introdotto dalla Direttiva 2014/41/UE, a cui è stata data attuazione nel nostro ordinamento con il d.gs. 21 giugno 2017, n. 108. Si deve altresì avere riguardo ai profili di transnazionalità delle attività di indagine connessi all'istituzione della Procura europea, con

[1] Sul sempre più frequente impiego, da parte dell'autorità giudiziaria, di strumenti investigativi a elevato contenuto tecnologico v. Cerqua Federico (2016), p. 96. In materia di prova digitale v. Di Paolo Gabriella (2013), pp. 736-762.
[2] Cfr. Pittiruti Marco (2017).

Regolamento 2017/1939, in relazione ai reati che offendano gli interessi finanziari dell'U.E.[3].

Deve peraltro ricordarsi come l'Unione europea abbia stipulato accordi con Stati terzi, quali U.S.A. e Giappone, in materia di assistenza giudiziaria[4].

Il presente lavoro, pur incentrato sugli strumenti normativi dell'Unione, accennerà altresì al progetto relativo a un secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica[5], anch'esso, come si vedrà, teso a superare alcune criticità relative all'accesso transfrontaliero alla prova digitale.

2. L'accesso transfrontaliero *all'electronic evidence* nell'ambito dell'Unione europea: le proposte di Regolamento e di Direttiva in materia di *European Production Order* e *European Preservation Order.*

Le recenti proposte di Regolamento[6] e di Direttiva[7], elaborate dalla Commissione, in materia di accesso transfrontaliero all'*electronic evidence,* esprimono l'esigenza di superare anche quei profili di criticità e quei rallentamenti caratterizzanti procedure pur "agili" quali quelle suindicate, adattando «i meccanismi di cooperazione all'era digitale, fornendo alle autorità giudiziarie e di contrasto gli strumenti per stare al passo con le attuali modalità di comunicazione dei criminali e combattere le forme moderne di criminalità», assicurando al contempo «forti meccanismi di tutela dei diritti fondamentali»[8]. Esse rispondono altresì agli auspici formulati nelle Conclusioni del Consiglio dell'Unione europea sul miglioramento della giustizia penale nel ciberspazio[9], del 2016, relativi all'incremento dell'efficienza dell'assistenza giudiziaria, al miglioramento della cooperazione tra le competenti autorità degli Stati membri e i prestatori di servizi stabiliti in Paesi terzi, nonché alla più chiara determinazione dei profili di territorialità legati allo svolgimento di indagini nel ciberspazio.

Le proposte appena menzionate, il cui iter formativo ha avuto inizio già con l'Agenda sulla sicurezza della Commissione del 2015 e ha subito una scossa soprattutto dopo gli attentati di Bruxelles del 2016[10], prendono in primo luogo atto del fatto che, oggi, oltre la metà dei procedimenti penali implica esigenze di accesso transfrontaliero alla prova digitale, comprensiva, quest'ultima, a titolo esemplificativo e secondo le indicazioni della stessa istituzione, di sms, e-mail, messaggistica scambiata attraverso apposite applicazioni, quali *Whatsapp*[11]. La definizione di "prova elettronica" è contenuta nella stessa proposta di Regolamento, all'art. 2, che riconduce a tale nozione «le prove conservate in formato elettronico dal prestatore di servizi o per suo conto al momento della ricezione del certificato di ordine europeo di produzione o di conservazione, consistenti nei dati conservati relativi agli abbonati, agli accessi, alle operazioni o al contenuto»[12].

Le citate proposte intendono quindi introdurre nuovi strumenti di cooperazione finalizzati all'acquisizione *dell'electronic evidence* secondo modalità rapide ed efficaci; si tratta, in

[3] V. in proposito Ruggeri (2018), p. 602.

[4] Ne sono un esempio la Decisione 2009/820/PESC del Consiglio, del 23 ottobre 2009, relativa alla conclusione, a nome dell'Unione europea, dell'accordo sull'estradizione tra l'Unione europea e gli Stati Uniti d'America e dell'accordo sulla mutua assistenza giudiziaria tra l'Unione europea e gli Stati Uniti d'America, e la Decisione 2010/616/UE del Consiglio, del 7 ottobre 2010, relativa alla conclusione dell'accordo tra l'Unione europea e il Giappone sull'assistenza giudiziaria reciproca in materia penale.

[5] Convenzione sulla criminalità informatica, aperta alla firma a Budapest il 23 novembre 2001.

[6] Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, 17 aprile 2018. Nella stessa Relazione illustrativa si dà atto della riconducibilità della scelta dello strumento del regolamento all'esigenza di predisporre -considerate le differenze anche significative ravvisabili tra gli ordinamenti dello Stato da cui provenga la richiesta e di quello di stabilimento del *service provider* - regole uniformi, necessarie quando vengano in considerazione procedure transfrontaliere, non apparendo opportuno lasciare agli Stati margini di apprezzamento nella loro attuazione.

[7] Proposta di Direttiva del Parlamento europeo e del consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali, 17 aprile 2018.

[8] Proposta di Regolamento, cit., 2.

[9] Conclusioni del Consiglio dell'Unione europea sul miglioramento della giustizia penale nel ciberspazio, 9 giugno 2016, in *www.data.consilium.europa.eu*.

[10] Cfr., per un commento alle due proposte in esame, Gialuz Mitja, Della Torre Jacopo (2018), p. 277 ss.; Pezzuto Raffaella (2019), pp. 57-88.

[11] Commissione europea, *E-evidence - cross-border access to electronic evidence,* in *www.ec.europa.eu.*

[12] V. Proposta di Regolamento, cit., art. 2.

primo luogo, dell'ordine europeo di produzione (*European Production Order*), tale da consentire l'instaurazione di un contatto diretto tra l'autorità giudiziaria di uno Stato membro e il *service provider* che non sia stabilito entro i confini propri della giurisdizione del primo, e in particolare con il suo rappresentante, obbligatoriamente designato da chi presti i propri servizi all'interno dell'Unione, ma non sia stabilito in uno Stato membro. A tale istituto dovrebbe inoltre affiancarsi l'ordine europeo di conservazione (*European Preservation Order*), tale da porre in capo al *provider* un obbligo di conservazione di dati ed elementi di prova per un certo periodo di tempo, nella prospettiva di una futura acquisizione degli stessi attraverso gli strumenti di assistenza giudiziaria previsti.

Non estraneo ai progetti normativi in esame – e anzi all'interno degli stessi espressamente contemplato – è l'intento di unire al perseguimento dei menzionati obiettivi di efficienza la previsione di un elevato livello di garanzie, connesse specialmente alla tutela della riservatezza dei dati conservati e trasmessi.

3. Ordine europeo di produzione, ordine europeo di conservazione, ordine europeo di indagine.

Operata tale premessa in ordine alle caratteristiche essenziali delle proposte normative in esame, appare opportuno procedere alla definizione dei rapporti con gli altri strumenti di cooperazione, in materia di ricerca e acquisizione della prova, già contemplati dal diritto dell'Unione europea, e in particolare con il recente istituto dell'ordine europeo di indagine (*European Investigation Order*)[13], introdotto dalla Direttiva 2014/41/UE, a cui è stata data attuazione nel nostro ordinamento con il d.lgs. 21 giugno 2017, n. 108, e considerato come la più avanzata disciplina in materia di raccolta transnazionale della prova mai adottata dal legislatore europeo, in quanto tale da rendere più rapida, snella e agevole la cooperazione tra Stati membri in materia[14].

In primo luogo, la stessa proposta di Regolamento oggetto di esame chiarisce[15] che la disciplina in materia di ordine europeo di indagine, applicabile ad ogni tipo di atto di indagine e probatorio[16], e quindi anche alla prova digitale, seppure non contenente apposite disposizioni relative a quest'ultima, rimarrà in vigore per tutti quei profili non specificamente disciplinati dalla nuova normativa; l'inopportunità di una modifica della Direttiva in materia di OEI è motivata proprio dall'estensione di quest'ultima a una pluralità di tipologie di atti probatori.

Invero, a titolo esemplificativo, con riguardo alle informazioni oggetto di acquisizione per le finalità della giustizia penale, il nuovo disegno normativo si riferisce espressamente ai soli dati – considerati in una prospettiva "statica" - conservati dal *provider,* e non anche alle intercettazioni di flussi di comunicazioni, che continuano pertanto a rientrare nell'ambito di applicazione delle disposizioni in materia di ordine europeo di indagine[17].

Giova altresì ricordare la possibile operatività, anche rispetto ai reati informatici di cui all'art. 51, comma 3-*quinquies,* c.p.p., delle disposizioni in materia di squadre investigative comuni[18].

[13] Di seguito indicato anche come "OEI".
[14] Allegrezza Silvia, Mosna Anna, Nicolicchia Fabio (2016), pp. 185-186.
[15] In questo senso la Relazione illustrativa della proposta di Regolamento.
[16] V. il considerando n. 6 della Direttiva, che, nel richiamare il Programma di Stoccolma del Consiglio UE del 10-11 dicembre 2009, fa riferimento all'auspicata «creazione di un sistema globale in sostituzione di tutti gli strumenti esistenti nel settore, compresa la decisione quadro 2008/978/GAI del Consiglio, che contempli per quanto possibile tutti i tipi di prove, stabilisca i termini di esecuzione e limiti al minimo i motivi di rifiuto». L'art. 3 del medesimo atto normativo specifica che non rientrano nell'ambito di applicazione della disciplina in materia di OEI solo l'istituzione di una squadra investigativa comune egli atti di indagine dalla stessa compiuti. Proprio in ragione dell'aspirazione di completezza riferibile alla normativa in materia di OEI, essa ha sostituito la Convenzione europea di assistenza giudiziaria del 1959 e i relativi protocolli, la Convenzione di applicazione dell'accordo di Schengen del 1990, la Convenzione relativa all'assistenza giudiziaria in materia penale dell'Unione del 2000, recepita dal d. lgs. 5 aprile 2017, n. 52, e la decisione-quadro 2003/577 sul sequestro probatorio. Lo strumento della rogatoria continua tuttavia a trovare applicazione nei rapporti con gli Stati membri che non abbiano attuato la Direttiva (Irlanda e Danimarca) e con gli Stati non U.E.: v. Belfiore Rosanna (2015), p. 3289; Daniele Marcello (2017), p. 208; Mangiaracina Annalisa (2018), p. 159.
[17] V. in particolare gli artt. 23-24 e 43-44 del decreto legislativo di attuazione della Direttiva sull'OEI, in materia di "ordine di intercettazione" rispettivamente ricevuto ed emesso dall'autorità giudiziaria italiana. Sul tema, Nocera Fabio (2018), pp. 149-168.
[18] Disciplinate dalla decisione quadro 2002/465/GAI, attuata nell'ordinamento italiano con il d.lgs. 15 febbraio 2016, n. 34.

4. Le caratteristiche fondamentali delle proposte normative.

4.1. *Dal mutuo riconoscimento al contatto diretto con il privato stabilito in altra giurisdizione.*

La proposta di Regolamento sugli ordini europei di produzione e conservazione, al pari delle normative in materia di ordine europeo di indagine e di squadre investigative comuni, è dichiaratamente ispirata al principio del mutuo riconoscimento, di cui all'art. 82 del Trattato sul Funzionamento dell'Unione europea[19]. Difatti – sebbene, con riferimento all'ordine europeo di indagine, si sia posto in luce[20] come tale principio non risulti integralmente attuato, in ragione della previsione da parte della Direttiva, e del decreto di attuazione, di motivi di non riconoscimento dell'OEI o di rinvio dello stesso – lo strumento di cooperazione da ultimo indicato è tale da comportare un diretto contatto tra le autorità degli Stati membri, in assenza, come detto, dell'intervento di istituzioni centrali, frequentemente fonte di ritardi e inefficienze[21].

Nel caso delle squadre investigative comuni, si configura addirittura l'operatività della squadra, all'interno di un determinato Stato membro, alla stregua di autorità del medesimo Stato[22].

Pertanto, il profilo realmente innovativo dell'ordine europeo di produzione e dell'ordine europeo di conservazione è costituito dalla previsione di un contatto diretto tra l'autorità giudiziaria di uno Stato membro e il privato stabilito in altro Stato membro – identificabile, ai sensi dell'art. 7 della proposta di Regolamento, con il rappresentante designato dal prestatore di servizi o con un qualsiasi stabilimento dello stesso nell'ambito territoriale dell'Unione - essendo l'intervento dell'autorità competente del Paese di stabilimento meramente eventuale, e subordinato all'inottemperanza al provvedimento. Quest'ultimo, infatti, emesso o convalidato da un'autorità giudiziaria di uno Stato membro, è diretto, in assenza di intermediazioni, al *service provider;* a tale nozione si riconducono «i prestatori di servizi di comunicazione elettronica, i prestatori di servizi della società dell'informazione per i quali la conservazione dei dati è una componente propria del servizio fornito all'utente, compresi i *social network* nella misura in cui non possono essere considerati servizi di comunicazione elettronica, i mercati online che agevolano le operazioni tra utenti (come consumatori o imprese) e altri prestatori di servizi di *hosting*, e i prestatori di servizi di nomi di dominio internet e di numerazione»[23].

Significativa è la rilevanza attribuita ai sistemi di *cloud,* caratterizzati dal fatto che il *provider* non necessita di essere stabilito o di disporre di *server* in ogni giurisdizione, potendo invece avvalersi di un'amministrazione centralizzata e di sistemi decentrati per la prestazione dei servizi e l'accesso ai dati. Pertanto, si estende l'ambito di applicazione della proposta di Regolamento a «servizi *cloud* e altri servizi di *hosting* che forniscono una vasta gamma di risorse informatiche, quali reti, *server* o altre infrastrutture, mezzi di conservazione, *app* e servizi che permettono di conservare dati a diversi scopi»[24]. Risultano invece escluse quelle attività nel cui ambito la conservazione dei dati rivesta un rilievo puramente accessorio, quali la prestazione di servizi giuridici, ingegneristici o contabili a distanza[25].

Si pongono in proposito, tuttavia, alcune questioni problematiche, sebbene la proposta valorizzi il ruolo dell'intervento dell'autorità giudiziaria in sede di emissione o convalida dell'or-

[19] V. Belfiore Rosanna (2015), p. 3288.
[20] Sulle ipotesi di mutuo riconoscimento "puro" contemplate dalla Direttiva in materia di OEI v. *ivi,* 3292-3293.
[21] Cfr. Camaldo Lucio (2014), "La direttiva sull'ordine europeo di indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione", *Diritto penale contemporaneo*.
[22] V., sul tema, Colaiacovo Guido (2017), pp. 169 ss.
[23] Proposta di Regolamento, cit., considerando n. 16. Secondo la definizione di cui all'art. 2, deve intendersi per *service provider* «la persona fisica o giuridica che fornisce una o più delle seguenti categorie di servizi: (a) servizi di comunicazione elettronica come definiti all'articolo 2, punto 4, della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche]; (b) servizi della società dell'informazione come definiti all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio44, per i quali la conservazione dei dati è una componente propria del servizio fornito all'utente, tra cui i social network, i mercati online che agevolano le operazioni tra utenti e altri prestatori di servizi di hosting; (c) servizi di nomi di dominio internet e di numerazione IP, quali i prestatori di indirizzi IP, i registri di nomi di dominio, i registrar di nomi di dominio e i connessi servizi per la privacy o proxy».
[24] *Ivi,* considerando n. 16.
[25] *Ibidem.*

dine, che dovrebbe assicurare anche il rispetto dei principi di necessità e proporzionalità. Le criticità prospettabili sono connesse in particolare alla valutazione, ad opera del privato, di legittimità dell'ordine e della conseguente necessità di darvi effettivamente seguito. Invero, la proposta prevede ragioni di legittima opposizione all'esecuzione dell'ordine piuttosto circoscritte[26] - secondo una scelta da ritenersi opportuna in quanto consente, coerentemente peraltro con la logica propria del mutuo riconoscimento, il perseguimento di quegli obiettivi di celerità ed efficienza che rischierebbero, diversamente, di essere frustrati - ma al tempo stesso definite in termini non sempre specifici e pregnanti. Basti pensare, al riguardo, ai riferimenti alla manifesta violazione delle previsioni della Carta dei diritti fondamentali dell'Unione europea e alla manifesta arbitrarietà dell'ordine[27].

Non possono pertanto escludersi difficoltà applicative in capo ai privati destinatari dei provvedimenti, potenzialmente di ostacolo al raggiungimento degli setessi scopi di efficienza perseguiti, pur dovendosi considerare che la proposta di Direttiva in materia di *electronic evidence* dispone, come si vedrà, la designazione ad opera dei prestatori di servizi di soggetti i quali sarebbero specificamente preposti alla ricezione e all'esecuzione dei provvedimenti disciplinati dal Regolamento, e pertanto presumibilmente dotati di una certa competenza e specializzazione.

Un ulteriore correttivo è rappresentato dalla disposizione relativa all'intervento, nell'ipotesi di rifiuto da parte del destinatario di ottemperare al provvedimento, della competente autorità del Paese di esecuzione, la quale potrà valutare la sussistenza delle condizioni ostative individuate dal Regolamento, nonché far valere l'esistenza di interessi ulteriori, tipicamente statali, e individuati nell'operatività di un'immunità o di un privilegio ai sensi del proprio diritto interno, o l'incidenza della divulgazione dei dati su interessi fondamentali dello Stato, quali la sicurezza e la difesa nazionali. In caso di avvio da parte dell'autorità da ultimo indicata della procedura di esecuzione, le medesime ragioni di rifiuto potranno inoltre essere fatte valere dinanzi alla stessa[28].

4.2. *I destinatari degli ordini europei di produzione e di conservazione.*

I destinatari dei provvedimenti sopra indicati – profilo specificamente oggetto della proposta di Direttiva – si individuano quindi nei rappresentanti legali appositamente designati dai prestatori di servizi per l'acquisizione delle prove; qualora questi non ottemperino, l'ordine dovrebbe essere trasmesso a un qualsiasi stabilimento del prestatore di servizi all'interno dell'U.E.[29], dovendo intendersi come tale, ai sensi dell'art. 2 della proposta, «l'esercizio effettivo di un'attività economica a tempo indeterminato con un'infrastruttura stabile a partire dalla quale viene svolta l'attività di prestazione di servizi, o l'infrastruttura stabile a partire dalla quale l'attività è gestita».

Le disposizioni proposte rispondono a una questione di particolare importanza nella materia considerata, quella dei diversi criteri utilizzati dagli Stati membri per l'affermazione della loro giurisdizione sui prestatori di servizi, e che possono consistere nel luogo di stabilimento,

[26] Secondo l'art. 14, par. 4, della proposta di Regolamento, «il destinatario può opporsi all'esecuzione dell'ordine europeo di produzione solo per uno dei seguenti motivi: (a) l'ordine europeo di produzione non è stato emesso o convalidato da un'autorità di emissione conformemente all'articolo 4; (b) l'ordine europeo di produzione non è stato emesso in relazione a un reato di cui all'articolo 5, paragrafo 4; (c) il destinatario non ha potuto ottemperare all'EPOC per impossibilità materiale o forza maggiore o perché l'EPOC contiene errori manifesti; (d) l'ordine europeo di produzione non riguarda dati conservati dal prestatore di servizi o per suo conto al momento della ricezione dell'EPOC; (e) il servizio esula dall'ambito di applicazione del presente regolamento; (f) dalle sole informazioni contenute nell'EPOC risulta che esso viola manifestamente la Carta dei diritti fondamentali dell'Unione europea o che è manifestamente arbitrario». Ai sensi del successivo par. 5, «il destinatario può opporsi all'esecuzione dell'ordine europeo di conservazione solo per i seguenti motivi: (a) l'ordine europeo di conservazione non è stato emesso o convalidato da un'autorità di emissione conformemente all'articolo 4; (b) il prestatore di servizi non ha potuto ottemperare all'EPOC-PR per impossibilità materiale o forza maggiore o perché l'EPOC-PR contiene errori manifesti; (c) l'ordine europeo di conservazione non riguarda dati conservati dal prestatore di servizi o per suo conto al momento della ricezione dell'EPOC-PR; (d) il servizio esula dall'ambito di applicazione del presente regolamento; (e) dalle sole informazioni contenute nell'EPOC-PR risulta che esso viola manifestamente la Carta dei diritti fondamentali dell'Unione europea o che è manifestamente arbitrario».

[27] A titolo esemplificativo, la Relazione illustrativa della proposta di Regolamento riconduce alla «manifesta arbitrarietà» l'ordine «che chieda la produzione di dati relativi al contenuto riguardanti una categoria indeterminata di persone in un'area geografica o che non ha alcun collegamento concreto con un procedimento penale», in quanto lo stesso «ignorerebbe in modo manifesto le condizioni per l'emissione dell'ordine europeo di produzione previste dal regolamento e ciò sarebbe evidente già dal contenuto del certificato».

[28] V. par. 1, 2, 6, 7 del citato art. 14.

[29] Così dispone l'art. 7 della proposta di Regolamento.

in quello di prestazione del servizio o di ubicazione dei dati o in una combinazione degli stessi. Pertanto, l'introduzione di norme armonizzate che consentano alle competenti autorità dei diversi Paesi di conseguire gli elementi di prova digitali anche da un prestatore di servizi non rientrante nella loro giurisdizione, finanche stabilito all'esterno dell'UE, e di conoscere con certezza quale sia il soggetto a cui potere inoltrare l'ordine, appare particolarmente opportuna, in assenza, al momento, di un'auspicabile maggiore uniformità di criteri per la determinazione della giurisdizione degli Stati.

Lo stato di frammentazione giuridica esistente si ritiene invero pregiudizievole per gli stessi prestatori di servizi: «Attualmente gli Stati membri hanno approcci diversi per quanto riguarda gli obblighi imposti ai prestatori di servizi, specialmente nei procedimenti penali. La frammentazione riguarda soprattutto le prove elettroniche, dal momento che alcuni prestatori di servizi conservano informazioni che possono essere utili per l'indagine e il perseguimento di reati. Tale frammentazione crea incertezza giuridica per i soggetti coinvolti e può sottoporre i prestatori di servizi a obblighi e regimi sanzionatori differenti e talvolta in conflitto tra loro a tale riguardo, a seconda del fatto che forniscano i loro servizi a livello nazionale, a livello transnazionale all'interno dell'Unione o al di fuori dell'Unione. Per ridurre gli ostacoli alla libera prestazione di servizi, la direttiva rende obbligatorio per i prestatori di servizi designare un rappresentante legale nell'Unione incaricato di ricevere decisioni volte ad acquisire prove emesse dalle autorità nazionali competenti nei procedimenti penali, ottemperare a tali decisioni e farle eseguire. La riduzione degli ostacoli che ne conseguirebbe migliorerebbe il funzionamento del mercato interno in modo coerente con lo sviluppo di uno spazio comune di libertà, sicurezza e giustizia»[30].

Si deve comunque precisare che la proposta Direttiva si configura quale applicabile ai prestatori di servizi i quali non si limitino a rendere fruibile il servizio all'interno dell'Unione, bensì abbiano un "collegamento sostanziale" con quest'ultima, da intendersi come disponibilità di uno stabilimento all'interno dell'Unione stessa, o di un numero significativo di utenti in uno o più Stati membri, o come orientamento dell'attività verso uno o più Stati membri, desumibile da una varietà di elementi tra loro eterogenei, che vanno dall'uso della lingua o della moneta dello Stato, alla disponibilità di una "*app*" nell' "*app store*" nazionale, alla pubblicità locale, alla gestione dei rapporti con la clientela. Precisa la Relazione illustrativa che «il criterio del collegamento sostanziale dovrebbe inoltre considerarsi soddisfatto qualora il prestatore di servizi diriga le sue attività verso uno o più Stati membri, come previsto all'articolo 17, paragrafo 1, lettera c), del regolamento (UE) n. 1215/2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale»[31].

L'obbligo di nomina del rappresentante in uno Stato membro in cui il service provider sia stabilito o presti servizi è volto ad evitare scelte "strategiche" del Paese di riferimento, in base, ad esempio, alle sanzioni previste in caso di inottemperanza al provvedimento conseguente all'esperimento della procedura di esecuzione.

Significativa è altresì la presa d'atto[32] dell'esistenza di servizi quali quelli di *hosting* o *software*, tali da comportare la conservazione dei dati all'interno di un'infrastruttura affidata dal *.provider* a una diversa società. In tal caso, salvo che sia inopportuno procedere secondo tale modalità per ragioni di potenziale compromissione delle indagini, l'accesso alla prova elettronica dovrebbe intervenire mediante il coinvolgimento della società stessa. Potranno tuttavia trovare applicazione, in questo caso, strumenti diversi rispetto a quelli oggetto del Regolamento – quali, a titolo esemplificativo, l'ordine europeo di indagine - essendo gli ordini europei di produzione e conservazione riservati ai soggetti qualificabili come "prestatori di servizi".

La designazione di soggetti specificamente preposti alla gestione degli ordini di trasmissione o conservazione di elementi che rivestano rilievo probatorio in procedimenti penali può ritenersi apprezzabile, in quanto tale da agevolare – secondo gli auspici degli stessi redattori della proposta normativa – le autorità competenti nell'individuazione dei destinatari dei provvedimenti emessi, coerentemente con la rapidità che deve contraddistinguere le indagini implicanti l'accesso all'*electronic evidence,* e da arginare le difficoltà incontrate dagli stessi prestatori di servizi nella risposta alle richieste ricevute, invero sempre più frequenti[33].

L'obbligo posto in capo ai prestatori di servizi all'interno dell'Unione di designare rappre-

[30] Così la Relazione illustrativa della proposta.
[31] *Ivi*, 9.
[32] V. in tal senso l'art. 5 della medesima proposta.
[33] V. la Relazione illustrativa della citata proposta di Direttiva.

sentanti è peraltro già previsto da alcune norme in particolari settori, tra cui il Regolamento generale sulla protezione dei dati personali 2016/679[34] e la Direttiva (UE) 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione[35].

Con riguardo al modello del contatto diretto con i privati prestatori di servizi, deve altresì ricordarsi come, pur rivestendo la cooperazione con tali soggetti, nel diverso contesto del Consiglio d'Europa, una rilevanza particolare ai sensi delle previsioni della Convenzione di Budapest sulla criminalità informatica del 2001, non sia ancora contemplata espressamente l'ipotesi di un contatto diretto con il privato stabilito al di fuori della giurisdizione dello Stato procedente. Proprio nella direzione da ultimo indicata, come si dirà, va quindi il progetto di secondo protocollo addizionale alla Convenzione; nondimeno, si è rilevato come nella prassi non siano infrequenti le richieste di fornitura di dati e informazioni rivolte da uno Stato al privato straniero, e rimesse alla volontaria scelta di collaborazione di quest'ultimo. Si registra, in particolare, una significativa tendenza dei *service providers* stabiliti negli Stati Uniti e in Irlanda a fornire spontaneamente alle autorità di altri Paesi gli elementi di rilievo probatorio[36], seppure a certe condizioni quali il fatto che, negli U.S.A., non si tratti di dati relativi al "contenuto".

4.3. *I tempi delle procedure.*

Una delle ragioni principali che si sono poste alla base della proposta in esame è rappresentata dalla riduzione dei tempi legati allo svolgimento di procedure pur "agili", quali quella dell'ordine europeo di indagine. In relazione a quest'ultimo, invero, in via generale la decisione sul riconoscimento e l'esecuzione dell'ordine deve essere adottata dall'autorità di esecuzione entro trenta giorni dalla ricezione dell'OEI, e l'esecuzione stessa deve avere luogo «senza ritardo», e comunque nel termine di novanta giorni dalla decisione stessa, salve le eccezioni contemplate dalla norma, nonché le proroghe ammesse per particolari motivi[37].

Significativamente più contenuti appaiono invece i tempi legati all'esecuzione degli ordini di produzione e conservazione, fissati dall'art. 9 della proposta di Regolamento in dieci giorni, riducibili fino a sei ore nei casi di urgenza.

4.4. *Profili attinenti alla tutela dei diritti.*

Analogamente a quanto previsto in materia di ordine europeo di indagine[38], si subordina l'operatività dei nuovi strumenti al rispetto dei principi di necessità e di proporzionalità.

Può sul punto ricordarsi che la normativa di attuazione delle disposizioni europee in materia di OEI, in tal senso discostandosi dall'orientamento della giurisprudenza di Strasburgo, che rimette alle autorità nazionali il bilanciamento tra i diversi interessi che entrano in gioco

[34] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), art. 27.

[35] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione; il relativo art. 18 prevede che il prestatore di servizi digitali no stabilito nell'U.E., ma che presti servizi al suo interno, si consideri stabilito nello Stato membro nel cui ambito ha designato il proprio rappresentante.

[36] Allegrezza Silvia (2018), p.150.

[37] Secondo la normativa in materia di ordine europeo di indagine (v. in particolare l'art. 12 della citata Direttiva 2014/41/UE), l'autorità di emissione può comunque rappresentare a quella di esecuzione l'esistenza di circostanze, legate a termini procedurali, gravità del reato o «altre circostanze particolarmente urgenti», che rendono necessario svolgere le attività considerate in tempi più rapidi, o eseguire l'OEI in una determinata data.

[38] L'art. 6 della citata Direttiva 2014/41/UE subordina l'emissione dell'ordine a una valutazione di necessità e di proporzionalità dello stesso, tenuto conto dei diritti dei soggetti sottoposti a procedimento. Il considerando n. 11 riferisce inoltre la valutazione di proporzionalità, al pari di quella di necessità, tanto alla prova, quanto all'atto di indagine funzionale all'acquisizione degli elementi di prova, quanto, ancora, all'emissione di un OEI al fine di conseguire la partecipazione di un altro Stato al medesimo atto, precisando altresì che l'autorità di esecuzione dovrebbe disporre della facoltà di porre in essere un atto meno intrusivo di quello richiesto, qualora esso consenta di conseguire risultati analoghi. Parte della dottrina ha espresso un orientamento critico rispetto alla prevista possibilità che l'autorità di esecuzione operi un'inedita consultazione dell'autorità di emissione, quando ritenga non rispettato il requisito di proporzionalità, in quanto si è osservato che tale vaglio è tale da introdurre, di fatto, nuove ipotesi di rifiuto, in contrasto con l'ispirazione della normativa in considerazione al principio del mutuo riconoscimento: in questo senso Belfiore Rosanna (2015), pp. 3292-3293.

quando sia necessario compiere una determinata attività investigativa, specifica i criteri secondo cui la valutazione di proporzionalità deve operare[39]. Essi attengono, in particolare, ai sensi dell'art. 8 d.lgs. 108/2017, alla possibilità di ritenere giustificato il sacrificio dei diritti dell'imputato, o della persona sottoposta alle indagini o comunque coinvolta dal compimento dell'atto richiesto, alla luce delle esigenze investigative e probatorie del caso concreto, tenuto conto della gravità del reato per cui si procede e della pena per lo stesso stabilita. Si potrebbe quindi immaginare, in proposito, un riferimento, quantomeno indicativo, a tali criteri anche ai fini della valutazione di necessità e proporzionalità dei nuovi provvedimenti proposti; la considerazione della gravità dell'illecito, nella valutazione di proporzionalità operata dall'autorità di emissione, è peraltro menzionata nella Relazione illustrativa della proposta di Regolamento.

Se, inoltre, in via generale, la normativa in materia di OEI sancisce la necessità di assicurare protezione ai diritti della persona sottoposta a procedimento, richiedendo altresì la tutela dei principi fondamentali dell'ordinamento giuridico dello Stato di esecuzione e imponendo il rispetto dei diritti difensivi e dei principi del giusto processo nell'ambito del processo celebrato nello Stato di emissione[40], la proposta in esame ribadisce l'operatività dei principi stessi, riconoscendo una primaria rilevanza, in ragione del suo più ristretto ambito di applicazione, alla salvaguardia della riservatezza dei dati.

Emerge quindi confermata la centralità nel diritto europeo del principio di proporzionalità: secondo quanto si è osservato, «la vera cifra che caratterizza quest'ultimo e che disegna una diversa concezione di legalità a forte componente "giudiziale" è infatti rappresentata da quel bilanciamento di valori e da quelle modulazioni applicative che si esprimono in modo precipuo nel canone di proporzionalità»[41].

Si premette comunque la potenziale incidenza dei provvedimenti oggetto delle norme citate su una pluralità di situazioni soggettive facenti capo ai diversi soggetti coinvolti: «diritti delle persone fisiche ai cui dati è previsto l'accesso: il diritto alla protezione dei dati personali; il diritto al rispetto della vita privata e familiare; il diritto alla libertà di espressione; il diritto alla difesa; il diritto a un ricorso effettivo e a un giudice imparziale; i diritti del prestatore di servizi: il diritto alla libertà d'impresa; il diritto a un ricorso effettivo; i diritti di tutti i cittadini: il diritto alla libertà e alla sicurezza»[42]. Analogamente a quanto previsto in relazione all'OEI, la proposta sancisce, in via generale, l'esigenza di rispetto dei principi fondamentali in materia penale e di processo penale, quali il diritto ad un equo processo, garantito dall'art. 6 CEDU e dagli artt. 47 e 48 della Carta dei diritti fondamentali dell'Unione europea; torna inoltre il rinvio alle direttive europee in materia di garanzie difensive, comune ad altri strumenti di cooperazione in ambito europeo[43].

Significativa è altresì la valorizzazione delle esigenze di tutela della libertà di prestazione di servizi dei soggetti i quali svolgano attività implicanti, quale aspetto non secondario, la conservazione dei dati che rendano possibile risalire all'identità dell'utente, ovvero alle caratteristiche "estrinseche" o di contenuto delle operazioni; l'attenzione prestata a tali istanze si riflette par-

[39] Trogu Mauro (2018), p. 1030. Cfr., nel senso dell'auspicio di una certa «tipizzazione» di determinati modelli di bilanciamento ad opera della Corte di giustizia, Kostoris Roberto E. (2018), p. 1448. L'Autore pone in luce la centralità del principio di proporzionalità, in quanto tale da consentire, pur in un contesto «fluido» quale quello europeo, un rilevante strumento di controllo dell'operato del giudice.

[40] V. l'art. 15 della Direttiva 2014/41/UE. Il rispetto dei principi fondamentali dell'ordinamento dello Stato di esecuzione rappresenta un correttivo al criterio della *lex loci:* cfr. Camaldo Lucio (2014). In materia di squadre investigative comuni, si è rilevato come il criterio della *lex loci*, sancito dall'art. 1, par. 3, lett. b) della decisione quadro, sia contemperato dalle previsioni che subordinano l'utilizzabilità dell'atto investigativo compiuto all'estero al rispetto delle regole processuali proprie dell'ordinamento giuridico ospitante, consentendo di salvaguardare le esigenze legate al rispetto dei diritti dei soggetti sottoposti a procedimento penale. Con riferimento, infine, alla Procura europea, si può evidenziare come, secondo le previsioni del Regolamento istitutivo, l'applicazione delle normative nazionali intervenga in relazione a tutti quegli aspetti che non siano disciplinati dall'atto europeo, e come una rilevanza centrale rivesta la struttura "decentrata" del medesimo organo, operante per lo più attraverso i procuratori delegati titolari delle indagini relative a fatti commessi nell'ambito del loro territorio, implicanti il compimento di atti che si svolgeranno essenzialmente secondo le regole proprie dello Stato di riferimento. Il criterio della possibilità di adottare il provvedimento in una situazione interna analoga nello Stato di emissione è sancito anche dall'art. 5 della proposta di Regolamento.

[41] Kostoris Roberto E. (2018), p. 1448.

[42] V. la Relazione illustrativa della proposta di Regolamento.

[43] Si tratta, in particolare, della Direttiva 2010/64/UE sul diritto all'interpretazione e alla traduzione nei procedimenti penali, della Direttiva 2012/13/UE sul diritto a ricevere informazioni relative ai diritti e all'accusa e ad accedere al fascicolo, della Direttiva 2013/48/UE relativa al diritto di avvalersi di un difensore e di comunicare con familiari al momento dell'arresto e della detenzione, della Direttiva 2016/343 sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo, della Direttiva 2016/800 sulle garanzie procedurali per i minori e la direttiva 2016/1919 sull'ammissione al patrocinio a spese dello Stato per indagati e imputati nell'ambito di procedimenti penali e per le persone ricercate nell'ambito di procedimenti di esecuzione del mandato d'arresto europeo. Si può ricordare come, salvo il riferimento nella normativa in materia di OEI ai principi e ai diritti fondamentali che si sono indicati, anche le disposizioni in materia di Procura europea operino un rinvio alle tutele riconducibili alla Carta dei diritti fondamentali dell'UE, alle direttive citate, nonché alle garanzie poste dagli ordinamenti nazionali.

ticolarmente nella proposta di Direttiva, volta espressamente, tra l'altro, a delineare un quadro normativo chiaro e uniforme in materia di obblighi di cooperazione dei *service providers,* e di modalità di ottemperanza ai relativi ordini giudiziali.

Venendo quindi al profilo centrale della riservatezza dei dati oggetto degli ordini di produzione e conservazione, l'art. 2 della proposta di Regolamento, coerentemente con quanto previsto negli ordinamenti di numerosi Stati membri, opera una distinzione tra gli stessi sulla base della loro eventuale attinenza al "contenuto"; più specificamente, si individuano, quali categorie di informazioni suscettibili di acquisizione a scopo probatorio, i dati relativi agli accessi[44], alle operazioni[45] e al contenuto[46], sebbene sia espressamente ricordato come esse ricadano, senza distinzioni, nell'ambito di applicazione della normativa europea in materia di tutela dei dati personali[47].

Può essere interessante rilevare come la stessa proposta dia atto della rilevanza della differenziazione delle categorie di informazioni di cui sopra anche in ordinamenti esterni all'Unione: ne costituisce un esempio quello statunitense, la cui normativa in materia consente ai *service providers* di condividere su base volontaria con le autorità di contrasto straniere i dati che non siano relativi al contenuto, salve limitate eccezioni[48].

Pertanto, in considerazione della diversa incidenza dei provvedimenti concernenti le varie categorie di dati sui diritti alla riservatezza, al rispetto della vita privata e familiare, alla libertà di espressione dei relativi titolari, si prevede, all'art. 5, che l'ordine europeo di produzione possa essere emesso per qualsiasi reato se concernente i dati relativi agli accessi e agli abbonati, e sia invece riservato all'accertamento di crimini di maggiore gravità, per cui la legge preveda la pena della reclusione superiore nel massimo a tre anni, o che rientrino nella categorie individuate dalla medesima disposizione , se riguardante i dati relativi al contenuto[49]. L'ordine europeo di conservazione può operare indipendentemente da limiti di gravità del reato per cui si procede; la mancata previsione di requisiti di tal genere rispetto a questa ipotesi, nonché, come detto, all'ordine di produzione che concerna dati relativi agli accessi e agli abbonati è stata oggetto di critica, in quanto, al pari dei presupposti di necessità e di proporzionalità, tale da comportare il rischio di un abuso di strumenti altamente "intrusivi" ad opera delle autorità di contrasto[50].

Secondo quanto espressamente indicato nella proposta di Regolamento[51], le relative prescrizioni si estendono anche ai dati criptati, analogamente a quanto è prescritto in tema di "ordine europeo di intercettazione". Evidente è la rilevanza di tali previsioni quando vengano in considerazione applicazioni, quali *Whatsapp* o *Skype,* che utilizzino tecniche di questo genere al fine di ostacolare l'accesso ai dati.

Il problema dell'interferenza tra le esigenze proprie dell'attività di accertamento di fatti penalmente illeciti e la tutela da assicurare ai diritti fondamentali dei soggetti coinvolti, tra cui la riservatezza dei dati conservati dal *service provider,* è emerso, in tempi piuttosto recenti, nel noto caso – seppure non implicante un accesso alla prova digitale di natura transfrontaliera – relativo alla richiesta rivolta ad Apple dall'Fbi nell'ambito delle investigazioni successive all'attentato terroristico di San Bernardino del dicembre 2015[52]. Come è noto, la società

[44] Si tratta dei dati, «tipicamente (…) registrati nell'ambito di una registrazione di eventi (in altre parole un *log server*) per indicare l'inizio e la fine di una sessione di accesso utente a un servizio», che consentono di risalire all'identità dell'utente – eventualmente a seguito dell'acquisizione dei dati relativi agli abbonati - per il tramite di un indirizzo IP o di altro identificatore che individui l'interfaccia di rete utilizzata per l'accesso (v. considerando n. 21 della proposta; per la relativa definizione, cfr. l'art. 2). A tali informazioni sono accostati, sotto il profilo del livello di incidenza sui diritti fondamentali, i dati relativi agli abbonati.

[45] Si tratta dei dati che rendono possibile risalire ai contatti dell'utente e al luogo in cui questo si trova (v. considerando n. 22 della proposta di Regolamento e, ancora, per la relativa definizione, il citato art. 2).

[46] L'art. 2 della proposta di Regolamento li identifica con «qualsiasi dato conservato in formato digitale, come testo, voce, video, immagine o suono, diverso dai dati relativi agli abbonati, agli accessi e alle operazioni».

[47] V. la proposta di Regolamento, cit., considerando n. 23.

[48] V., sul punto, il considerando n. 19 della proposta di Regolamento.

[49] Questi ultimi, come espressamente chiarito, sono «reati armonizzati» la cui prova è tipicamente disponibile solo in formato elettronico:) la decisione quadro 2001/413/GAI del Consiglio relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, ii) la direttiva 2011/92/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio e iii) la direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio. L'ordine può essere emesso anche per i reati elencati nella direttiva (UE) 2017/541 sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio.

[50] Gialuz Mitja, Della Torre Jacopo (2018), p. 293.

[51] Secondo il considerando n. 19 della proposta, i dati devono essere forniti indipendentemente dal fatto che siano criptati o meno.

[52] V. Signorato Silvia (2016), p. 198.

produttrice dell'*iPhone* ha rifiutato l'accoglimento della richiesta diretta alla modifica di una caratteristica propria del dispositivo, e tale da implicare la distruzione dei dati ivi contenuti a seguito di un certo numero di tentativi infruttuosi di inserimento del codice di blocco, sebbene in seguito gli investigatori siano riusciti comunque ad accedere alle informazioni archiviate nello *smartphone* interessato[53].

Sotto il diverso profilo della garanzia del diritto di difesa della persona a cui si riferiscono i dati acquisiti, l'art. 11 della proposta di Regolamento contiene previsioni espressamente[54] tese a contemperare le esigenze di salvaguardia dell'attività di indagine con quelle connesse alla tutela della riservatezza dei soggetti coinvolti dall'accesso ai dati, e che dovranno essere informati, se non dallo stesso *service provider*, comunque dall'autorità di emissione, quando non vi sia più pericolo di pregiudizio per le investigazioni, in conformità con l'art. 13 della Direttiva sulla protezione dei dati nelle attività di polizia e giustizia. Si prescrive in particolare, nella prospettiva dell'utile esperimento dei mezzi di impugnazione, l'informativa sui mezzi di ricorso disponibili. Le disposizioni di cui all'art. 11 della proposta in esame si ispirano, per espressa indicazione dei redattori[55], all'art. 19 della Direttiva in materia di ordine europeo di indagine. Quest'ultimo deve essere considerato congiuntamente al considerando n. 22 della medesima Direttiva 2014/41/UE, secondo cui lo Stato di esecuzione dovrebbe garantire mezzi di impugnazione almeno equivalenti a quelli previsti per atti interni analoghi[56].

Proseguendo nella trattazione di alcune delle questioni che possono ritenersi più significative sul piano del bilanciamento tra esigenze di effettività dell'attività investigativa e tutela dei diritti fondamentali, con riguardo ai provvedimenti di cui si propone l'introduzione, merita particolare attenzione la già rilevata[57] possibilità che gli ordini siano diretti a rappresentanti di *providers* che, pur prestando i propri servizi all'interno dell'Unione, siano stabiliti in Paesi terzi, i cui ordinamenti garantiscano un più elevato livello di tutela della riservatezza o di altri diritti fondamentali. Basti pensare al caso degli Stati Uniti, il cui *Electronic Communications Privacy Act (EPA)* vieta la divulgazione di dati relativi al contenuto, rientranti nell'ambito geografico di applicazione dello stesso, fatta eccezione per ipotesi limitate. Premesso che la questione dei rapporti con i *service providers* statunitensi sarà oggetto di apposita trattazione, si deve rilevare come il problema sia stato considerato dalle proposte normative in esame, le quali contemplano la possibilità che il destinatario dell'ordine di produzione, qualora ritenga l'ottemperanza allo stesso in contrasto con il diritto applicabile di un Paese terzo che vieti la divulgazione dei dati per motivi diversi da quelli di cui all'articolo 15, informi l'autorità di emissione dei motivi per non eseguire l'ordine conformemente alla procedura di cui all'art. 9, par. 5.

4.5. *I mezzi di impugnazione.*

La proposta di Regolamento elaborata dalla Commissione europea pone previsioni diverse in materia di impugnazioni, in relazione ai soggetti coinvolti dai provvedimenti adottati.

Per quanto concerne i prestatori di servizi, si può rinviare a quanto si è detto in precedenza in materia di opposizione all'ordine emesso dall'autorità straniera, con la precisazione per cui, qualora l'autorità dello Stato di esecuzione decida di dare corso all'ordine pur a fronte delle deduzioni del destinatario, è fatto salvo il diritto a un ricorso giurisdizionale nei confronti del provvedimento dell'autorità dello Stato di esecuzione.

In capo ai soggetti titolari dei dati, invece, l'art. 17 della proposta di Regolamento pone il diritto a un ricorso giurisdizionale nello Stato di emissione, seppure limitatamente all'ordine europeo di produzione, che è l'unico a comportare la divulgazione effettiva dei dati stessi. In senso critico rispetto a tale previsione si sono espressi peraltro i primi commentatori delle

[53] *Ibidem.*
[54] Cfr. la Relazione illustrativa, 21.
[55] *Ibidem.*
[56] Gli artt. 4 e 13 d.lgs. 108/2017 prevedono che nel nostro ordinamento il decreto di riconoscimento sia comunicato al difensore nel termine stabilito per l'avviso di cui ha diritto secondo la legge italiana; qualora le norme processuali stabiliscano il diritto all'assistenza all'atto di indagine, ma non al previo avviso, la comunicazione interviene contestualmente al compimento dell'atto stesso o subito dopo. L'impugnazione avverso il decreto di riconoscimento dell'ordine, che assume la forma dell'opposizione al g.i.p. del tribunale presso cui ha sede la procura della Repubblica che ha provveduto al riconoscimento, è ammessa entro cinque giorni dalla comunicazione: cfr. Trogu Mauro (2018), pp.1020 ss. e 1046 ss.
[57] V. *supra,* par. 4.1.

proposte normative in esame, i quali, ritenendo le stesse sbilanciate nella direzione del soddisfacimento delle esigenze repressive, più che in quella della tutela dei diritti fondamentali, hanno rilevato che anche la semplice indisponibilità di determinati dati che si riferiscono alla propria persona per un certo periodo di tempo è tale da tradursi in una limitazione di libertà tale da richiedere quantomeno la previsione di mezzi di impugnazione adeguati[58].

Sono comunque fatti salvi gli strumenti di ricorso previsti dagli atti normativi dell'Unione in materia di tutela dei dati personali. Si precisa altresì che «i termini o altre condizioni per la proposizione del ricorso sono uguali a quelli previsti in casi interni analoghi e sono applicati in modo da garantire alle persone interessate l'esercizio effettivo del ricorso»[59].

L'art. 17 della proposta specifica che il gravame dovrebbe essere proposto da indagati e imputati all'interno del procedimento penale, e dagli altri soggetti interessati avvalendosi degli strumenti previsti nello Stato di emissione. Sul punto, può rilevarsi come le previsioni considerate siano molto generali – e lo siano comprensibilmente, se si ha riguardo alle differenze normative rinvenibili in materia tra gli Stati membri - ma al tempo stesso possano implicare qualche difficoltà nell'individuazione dei mezzi di impugnazione esperibili nell'ordinamento interno, attesa la diretta applicabilità delle disposizioni del Regolamento.

Si potrebbe quindi ipotizzare, anche in questo caso, il riferimento a quanto stabilito dalla nostra legge processuale rispetto a casi interni analoghi, ossia alle previsioni in materia di impugnazione del provvedimento di sequestro probatorio di dati relativi a sistemi informatici o telematici, *ex* artt. 254-*bis* e 257 c.p.p., nell'ambito del procedimento penale aperto nello Stato di emissione.

Giova ricordare, sul punto, che la normativa di attuazione della Direttiva in materia di OEI, a fronte della disposizione di cui all'art. 14 relativa alla necessità che siano previsti mezzi d'impugnazione equivalenti a quelli disponibili in un caso interno analogo, all'art. 13 d.lgs. 108/2017 ha disciplinato un apposito strumento di contestazione anche del decreto di riconoscimento dell'ordine, consistente nell'opposizione al giudice per le indagini preliminari. La medesima Direttiva ha invece limitato la contestazione del provvedimento per motivi di merito all'esperimento di un'azione nello Stato di emissione dell'OEI.

5. La cooperazione con i *service providers* stabiliti in Stati terzi: il caso degli Stati Uniti.

Come si è avuto modo di osservare, le stesse proposte normative esaminate, pur introducendo le previsioni in materia di nomina di rappresentanti ad opera dei *providers* che forniscano il proprio servizio all'interno dell'U.E., prendono atto delle criticità riconducibili all'esigenza di accedere a dati detenuti da soggetti stabiliti in Paesi terzi, attese le possibili differenze normative riscontrabili tra gli ordinamenti di questi ultimi e quelli degli Stati membri, anche sotto il profilo della tutela della riservatezza e degli altri diritti fondamentali.

Si è già evidenziato il caso degli Stati Uniti, in cui la trasmissione dei dati relativi al "contenuto" è soggetta a limiti rigorosi. Nondimeno, si può anche osservare come proprio in tale Paese abbiano sede molti dei più importanti *Internet providers:* basti pensare a Facebook, Google, Twitter.

La possibilità di accesso ai dati detenuti da tali soggetti, ad opera delle autorità degli Stati membri dell'Unione, è stata in passato assicurata dal *Mutual Legal Assistance Agreement* stipulato tra U.S.A. e U.E., sebbene i tempi particolarmente significativi connessi allo svolgimento delle procedure di mutua assistenza si siano rivelati sovente incompatibili con le esigenze legate all'acquisizione di elementi probatori caratterizzati da estrema volatilità e suscettibili di modifica e alterazione. Pertanto, in sede di revisione dell'accordo, nel 2016, gli Stati membri erano stati incoraggiati a porre in essere contatti diretti con i *providers* statunitensi, al fine di conseguire gli obiettivi di accesso alla prova digitale. La collaborazione volontaria dei prestatori di servizi digitali era quindi andata configurandosi quale alternativa alla cooperazione giudiziaria tra le autorità competenti dei Paesi coinvolti., sebbene il carattere non doveroso della prima avesse determinato una gestione delle richieste ad opera dei relativi destinatari secondo un approccio casistico, o fondato su criteri dagli stessi autonomamente determinati.

[58] Gialuz Mitja, Della Torre Jacopo (2018), p. 292.
[59] V. l'art. 17 della proposta di Regolamento.

Si può penare, a tale ultimo proposito, alle linee guida elaborate da Facebook, Apple, Google[60].

Proprio le criticità sopra menzionate hanno quindi condotto la Commissione, nel febbraio 2019, a proporre due mandati negoziali, soggetti all'approvazione del Consiglio; essi concernono l'uno i rapporti con gli Stati Uniti, l'altro la partecipazione ai negoziati relativi al secondo Protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica, a cui si è fatto cenno e di cui si tratterà più ampiamente nel prossimo paragrafo[61].

Con riguardo all'auspicato accordo con gli Stati Uniti, esso tende alla creazione di regole comuni, tali da assicurare il superamento degli ostacoli alla cooperazione in materia di accesso alla *digital evidence* riconducibili alle differenze normative tra i Paesi interessati, nonché la sicurezza dei dati trasferiti e un elevato livello di tutela dei diritti fondamentali, coerentemente con la Carta dei diritti fondamentali dell'Unione europea, i principi generali del diritto dell'Unione e la giurisprudenza della Corte di giustizia[62]. Tali nuove disposizioni, nelle intenzioni della Commissione europea, dovrebbero costituire il completamento dell'*EU-U.S. Data Protection and Privacy Agreement*, stipulato nel 2017, nonché lo *U.S. Judicial Redress Act*.

Si pone infine in evidenza come la proposta di avvio di negoziati da parte della stessa Unione europea sia volta proprio a evitare la riproposizione di quella frammentazione normativa che deriverebbe dalla conclusione di singoli accordi bilaterali tra gli Stati Uniti, i diversi Stati membri dell'U.E. e Paesi terzi[63].

6. Il progetto di un secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica: cenni.

Si è appena avuto modo di osservare come la Commissione europea abbia proposto l'avvio di negoziati anche per il coinvolgimento dell'Unione europea nella stipula del secondo protocollo addizionale alla Convenzione di Budapest del 2001, ancora allo stadio di progetto normativo.

Invero, le nuove sfide ed esigenze legate all'accesso transfrontaliero all'*electronic evidence* hanno condotto gli Stati membri del Consiglio d'Europa a ricercare soluzioni, prima attraverso un apposito gruppo di lavoro operante dal 2012 al 2014, e poi, dal 2015 al 2017, per il tramite del *Cloud Evidence Group*[64].

Si può notare come gli obiettivi perseguiti mediante il progetto normativo in esame siano del tutto analoghi a quelli che ispirano le proposte recentemente sviluppate dalla Commissione europea: vengono in particolare in considerazione le esigenze di incremento della rapidità e dell'efficienza della cooperazione in materia di accesso alla prova digitale, da perseguire anche mediante l'instaurazione di forme dirette di contatto tra le autorità competenti dei Paesi che abbiano sottoscritto la Convenzione e il *service provider* stabilito in altro Stato parte.

Deve peraltro ricordarsi come la previsione di obblighi di collaborazione in capo ai prestatori di servizi, ma limitatamente a quelli rientranti nell'ambito della giurisdizione propria dello Stato precedente, era già una caratteristica propria della Convenzione, come testimoniano alcune norme del nostro ordinamento processuale, e in particolare quelle in materia di sequestro probatorio di cui all'art. 254-*bis* c.p.p.

[60] Si considerino, a titolo esemplificativo, i criteri predisposti da Facebook: «*With regard to requests from:- USA authorities, Facebook "disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712."- International requests, Facebook "disclose account records solely in accordance with our terms of service and applicable law. A Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account."*
Facebook Ireland Limited is a subsidiary of Facebook Inc. All users outside of the USA and Canada apparently have a contract with Facebook Ireland Limited. Under its "data policy", Facebook may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards» (v. Cybercrime Convention Committee (T-CY), *Criminal justice access to data in the cloud: Cooperation with "foreign" service providers*, 3 maggio 2016.

[61] Commissione europea, *Security Union: Commission recommends negotiating international rules for obtaining electronic evidence,* in www.europa.eu, 5 febbraio 2019.

[62] Commissione europea, *Questions and Answers: Mandate for the EU-U.S. cooperation on electronic evidence,* in www.europa.eu, 5 febbraio 2019.

[63] *Ibidem.*

[64] Council of Europe, *Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention,* in www.rm.coe.int, 19 marzo 2018.

7. Considerazioni conclusive.

In conclusione, può dirsi oggetto di una crescente attenzione, non solo nell'ambito dell'Unione europea, un nuovo modello di cooperazione tra gli Stati per l'acquisizione degli elementi di prova in formato elettronico, quello del contatto diretto tra le autorità che procedano per un determinato illecito e il prestatore di servizi – o il suo rappresentante o stabilimento – il quale detenga i dati al di fuori dell'ambito territoriale del Paese procedente.

I benefici in termini di rapidità ed efficienza che possono derivarne alle indagini sono senza dubbio apprezzabili, così come merita di essere considerato favorevolmente il tentativo di individuare una soluzione effettiva ad uno dei problemi più significativi della materia, costituito dai rapporti con Paesi terzi, le cui normative interne possono costituire un ostacolo alla messa a disposizione dei dati. Esigenze di uniformità delle disposizioni applicabili e di comparabilità dei rispettivi livelli di tutela dei diritti fondamentali si pongono in maniera sempre più pressante, e può ritenersi pertanto auspicabile la prosecuzione dell'Unione europea nel percorso che la avvicina, dopo alcuni sviluppi particolarmente significativi conosciuti dalla cooperazione giudiziaria in materia penale, e in conformità con il principio del mutuo riconoscimento, a un modello innovativo di svolgimento dell'attività investigativa oltre i confini nazionali.

Si rivela peraltro apprezzabile l'intento di coniugare le istanze relative all'efficacia dell'attività di raccolta degli elementi di prova con la garanzia di un elevato livello di tutela dei diritti fondamentali dei soggetti i quali siano, a vario titolo, dalla stessa coinvolti, sebbene non manchino alcuni elementi di criticità, secondo quanto si è avuto modo di osservare.

Le proposte normative considerate necessitano indubbiamente di chiarificazione, sotto alcuni profili, essendo ravvisabili taluni aspetti problematici, e potenzialmente fonti di incertezze, delle medesime – quali, a titolo esemplificativo, le previsioni concernenti la contestazione degli ordini e i mezzi di impugnazione - e persistendo il significativo ostacolo legato alle differenze normative rinvenibili tra i diversi Paesi, in merito a profili essenziali quali la stessa determinazione dell'assoggettamento di un determinato *provider* alla giurisdizione statale.

Il problema della disomogenea definizione dei criteri di attribuzione della giurisdizione, con il rischio di avvio di procedimenti in una pluralità di Paesi, continua ad essere di particolare serietà, in particolare in materia di reati informatici, anche in ragione – secondo quanto si è osservato – della scarsa adeguatezza, rispetto alle indagini informatiche, di previsioni quali quelle del nostro codice penale, che legano la potestà punitiva statale[65] alla commissione del fatto entro il territorio dello stesso, salvi i casi di procedibilità per illeciti commessi all'estero. Si è peraltro osservato[66] come la legge 18 marzo 2008, n. 48 non abbia recepito la norma di cui all'art. 22, par. 5, della Convenzione di Budapest, che ha previsto il «rimedio preventivo» della consultazione tra Stati al fine di stabilire la «competenza più appropriata per l'esercizio dell'azione penale».

Nondimeno, nella misura in cui i progetti considerati agevoleranno lo svolgimento di attività ormai implicate dalla maggioranza dei procedimenti penali, e purché si realizzi un coordinamento tra le normative riferibili ai diversi ambiti dell'Unione europea, della Convenzione di Budapest, degli accordi con i Paesi terzi, si tratta di innovazioni che possono essere guardate con favore.

Sarà altresì la futura evoluzione delle proposte elaborate dalla Commissione, e l'eventuale applicazione pratica degli istituti a consentire di valutare se, effettivamente, il nuovo modello del contatto diretto con il privato – che comunque non pregiudica gli altri strumenti di cooperazione esistenti, quali l'OEI – sia tale da non tradire le aspettative.

Bibliografia:

Aa. Vv. (2011), *Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici* (Forlì, Experta).

[65] Daniele Marcello (2011), *La prova digitale nel processo penale,* in *Riv. dir. proc.,* 2011, 2, 287.
[66] *Ibidem.*

Allegrezza Silvia (2018), "Prova scientifica e dimensione europea", in Canzio Giovanni, Luparia Luca (eds.), *Prova scientifica e processo penale,* (Padova, CEDAM), 117-157.

Allegrezza Silvia, Mosna Anna, Nicolicchia Fabio (2016), "L'acquisizione della prova all'estero e i profili transnazionali", in Canzio Giovanni, Cerqua Luigi Domenico, Luparia Luca (eds.), *Diritto penale delle società,* (Padova, CEDAM), pp. 157-192.

Belfiore Rosanna (2015), "Riflessioni a margine della Direttiva sull'ordine europeo di indagine penale", *Cassazione pen*ale, 2015, 9, 3288-3295.

Camaldo Lucio (2014), "La direttiva sull'ordine europeo di indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione", *Diritto penale contemporaneo*.

Cerqua Federico (2016), "Le indagini ad alta tecnologia per il contrasto della criminalità informatica", in Canzio Giovanni, Cerqua Luigi Domenico, Luparia Luca, *Diritto penale delle società,* (Padova, CEDAM), pp. 93-106.

Colaiacovo Guido (2017), "Nuove prospettive in tema di coordinamento delle indagini e cooperazione giudiziaria alla luce della disciplina delle squadre investigative comuni", *Rivista trimestrale Diritto penale contemporaneo*, 1, pp. 169-174.

Daniele Marcello (2017), "L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul d. lgs. n. 108 del 2017", *Diritto penale contemporaneo*, 7-8, pp. 208-215.

Daniele Marcello (2011), "La prova digitale nel processo penale", *Rivista di diritto processuale*, 2, pp. 283-298.

Di Paolo Gabriella (2013), "Prova informatica (diritto processuale penale)", in *Enciclopedia del diritto, Annali, VI*, (Milano, Giuffrè), pp. 736-762.

Gialuz Mitja, Della Torre Jacopo (2018), "Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali", *Diritto penale contemporaneo,* 5, pp. 277-294.

6.

Kostoris Roberto E. (2018), "Ordine di investigazione europeo e tutela dei diritti fondamentali", *Cassazione penale*, 5, pp. 1437-1449.

Mangiaracina Annalisa (2018), "L'acquisizione "europea" della prova cambia volto: l'Italia attua la Direttiva relativa all'ordine europeo di indagine penale. Commento a d.lg. 21 giugno 2017, n. 108", *Diritto penale e processo*, 2, p. 159.

Marchetti Maria Riccarda (2018), "Ricerca e acquisizione probatoria all'estero: l'ordine europeo di indagine", *Archivio penale*, 1S, p. 827.

Nocera Andrea (2018), "Il sindacato giurisdizionale interno in tema di ordine europeo di intercettazione", *Diritto penale contemporaneo,* pp. 149-168.

Pezzuto Raffaella (2019), "Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione", *Diritto penale contemporaneo,* 1, pp. 57-88.

Pittiruti Marco (2017), *Digital evidence e procedimento penale* (Torino, Giappichelli).

Ruggeri Stefano (2018), "Indagini e azione penale nei procedimenti di competenza della Procura europea", *Processo penale e giustizia*, 3, pp. 602-616.

Signorato Silvia (2016), "Tipologie e caratteristiche delle *cyber investigations* in un mondo globalizzato", *Rivista Trimestrale Diritto penale contemporaneo,* 3, pp.190-200.

Siracusano Francesco (2017), "La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione", *Processo penale e giustizia*, 1, p. 18.

Tinoco Pastrana Angel, "L'ordine europeo di indagine penale. Commento a Dir. UE 2014/41", *Processo penale e giustizia*, 2017, 2, pp. 342-359.

Trogu Mauro (2018), "Ordine europeo di indagine penale", in Marandola Antonella (editor), *Cooperazione giudiziaria europea in materia penale* (Milano, Giuffrè), pp. 1004-1101.

L'utilizzo dello *smartphone* alla guida nei delitti di omicidio e lesioni colpose stradali

El uso del smartphone al momento de conducir en los delitos de asesinato y lesiones culposas

The Usage of Smartphones While Driving and The Traffic-Related Crimes of Manslaughter and Personal Negligence-Based Injuries

Giacomo Maria Evaristi
Dottorando di ricerca presso l'Università di Camerino
giacomo.evaristi@unicam.it

Colpa | Culpa | Negligence

Abstracts

Il crescente fenomeno della distrazione tecnologica del conducente alla guida di veicoli ha reso necessario che, in caso di scontro con esiti lesivi di beni primari, si volgesse l'attenzione allo *smartphone* contestualmente ai rilievi descrittivi. Così alcune Procure della Repubblica hanno emanato direttive finalizzate a contenere abusi degli organi di polizia giudiziaria, senza pregiudicare l'accertamento delle responsabilità penale per i delitti di omicidio e lesioni colpose stradali. In questo quadro si rileva l'utilità del *file* di *log*, documento digitale auto-generato dal dispositivo che annota le operazioni di dialogo tra utente-apparecchio secondo sequenze temporali tracciando cronologicamente l'utilizzo compiutone dal conducente. I *file* di *log*, anche con riferimento alle applicazioni di messaggistica istantanea, hanno un *focus* investigativo limitato al se e quando vi è stato l'uso dello *smartphone* o della singola applicazione, impedendo una generalizzata indagine sulle informazioni salvate nel dispositivo. Ancora discusse risultano invece le modalità procedimentali di acquisizione dei dati informatici, per le quali il diritto vivente pare dimenticare il carattere volatile e alterabile della *digital evidence*.

El creciente fenómeno de la distracción tecnológica del conductor de vehículos ha tenido como consecuencia que, en caso de una colisión con resultados lesivos, la atención se dirija al Smartphone. Algunas fiscalías han elaborado directivas a fin de evitar abusos por parte de la policía, sin prejuzgar la responsabilidad penal del conductor. En este contexto, se evidencia la importancia del archivo de registro, documento digital generado por el propio dispositivo que anota las operaciones de dialogo entre el usuario y el aparato. El archivo de registro tiene una utilidad investigativa limitada a si y cuándo se usó el smartphone y la especifica aplicación, impidiendo por tanto una investigación general sobre las informaciones grabadas en el dispositivo. Todavía se discuten los métodos para adquirir datos informáticos, para los cuales el derecho parece olvidar la naturaleza volátil y alterable de la evidencia digital.

The increasing phenomenon of IT distractions for drivers made inevitable, in the event of accidents involving people, checking the smartphone in addition to other crash measurements. Some Italian Prosecutor Offices issued guidelines in order to avoid any abuse by the police, without prejudice to the assessment of criminal liability for the road/traffic-related offences of manslaughter and personal negligence-based injuries. In the said scenario, the log file can be useful, being a digital document self-generated by a device where all the operations performed with it by the driver are recorded over the time. The log files, even in instant messaging apps, have an investigation focus limited to if and when the smartphone or a single app were used, without an overall view of the information

storage. It is still controversial, in turn, how to acquire such data, especially because the case law seems to forget the volatility and unreliability of digital evidence.

Sommario

1. Premessa.

La circolazione stradale rientra nel gruppo di attività pericolose giuridicamente autorizzate per via del beneficio che la collettività ne trae dallo svolgimento[1].

In tale settore, l'ordinamento fissa uno stretto reticolo di norme a contenuto cautelare, sia generico che specifico[2], con l'obiettivo di eliminare o quantomeno ridurre il rischio di eventi lesivi, in particolare dei beni della vita e dell'integrità fisica dei consociati[3].

Tra le maggiori cause di incidenti stradali si evidenzia la c.d. distrazione tecnologica prodotta dall'utilizzo dello *smartphone* (o *tablet*) durante la marcia[4]: il conducente distoglie la propria attenzione dalla strada per taluni secondi, poiché intento ad operare sul dispositivo elettronico, finendo per perdere il controllo del proprio veicolo, ovvero non avendo la giusta prontezza nell'affrontare le situazioni della circolazione. In particolare, l'utilizzo dell'apparecchio radiotelefonico, in ragione dello sviluppo tecnologico che lo ha interessato negli ultimi anni, attrae l'attenzione per numerose possibilità di utilizzo, che inducono il conducente a spostare lo sguardo dal percorso, creando dei momenti di vuoto di dominio sull'autovettura.

Con riferimento al rilievo penale di tali condotte, si deve premettere che il legislatore nel 2016 ha affrancato le fattispecie di omicidio colposo e lesioni colpose stradali, al fine di costituire una adeguata risposta repressiva nei confronti delle condotte imprudenti alla guida dei veicoli[5]. All'interno di tali nuove fattispecie, speciali per specificazione, il legislatore è intervenuto a graduare il rimprovero attraverso la previsione di circostanze aggravanti c.d. indipendenti per le condotte che manifestano un maggior allarme sociale, contravvenendo le elementari disposizioni cautelari in materia di circolazione stradale[6].

La distrazione tecnologica alla guida costituisce una delle nuove sfide alla prevenzione penale, facendo perno sulla disposizione specifica dell'art. co. 173 co. 2 Codice della Strada, che vieta l'utilizzo di apparecchi radiotelefonici da parte di chi si trova alla guida del veicolo.

Poiché ai fini dello scrutinio in ordine alla integrazione di questa fattispecie colposa si richiede, tra l'altro, la prova della violazione della regola cautelare a contenuto specifico, il ganglio centrale dell'accertamento penale concerne propriamente se vi sia stato l'utilizzo del dispositivo alla guida negli attimi immediatamente precedenti l'evento naturalistico occorso. Si conferma così l'assunto della centralità, nel procedimento penale, della *digital evidence*, la quale non ha rilievo limitato ai soli reati digitali, bensì anche alle fattispecie ove il dispositivo elettronico è strumento, anche solo occasionale, di realizzazione della condotta tipica[7].

Tale esigenza di ricostruzione ed accertamento della dinamica dell'incidente automobilistico, può ricevere fondamentale supporto dai c.d. *file* di *log*. Invero, il sistema operativo o le singole applicazioni dell'apparecchio radiotelefonico annotano, con data ed orario, le attività compiute nell'interfacciarsi con il dispositivo. L'insieme delle suddette informazioni viene raggruppato ed ordinato temporalmente, secondo una scansione temporale precisa, all'interno del

[1] Mantovani (2015), p. 173.

[2] Si è posto in luce che le norme contenenti prescrizioni positive di condotta presentano comunque un contenuto ampio, sicché devono essere definite elastiche.

[3] Siamo dinanzi alle c.d. regole cautelari improprie, giacché il loro scopo è quello di contenere il livello di rischio entro un *range* di accettabilità, senza di bloccare ab origine lo svolgimento di una determinata attività lesiva come prescrivono le c.d. regola cautelari proprie). Su questa distinzione, si esprime P. Veneziani, (2003), p. 20 s.

[4] L'ISTAT svolge annualmente analisi dei dati sui sinistri stradali, indicando il numero di vittime o feriti che sono ascrivibili a tale circostanza. Le informazioni, relative al 2017, sono riportante nel seguente link: https://www.istat.it/it/files/2018/07/Incidenti-stradali_2017.pdf

[5] La ragione della scelta di politica criminale deve essere ricondotta alla trasformazione del contenuto del *dolo eventuale*. Il superamento della teoria dell'accettazione del rischio, rimpiazzata dalla c.d. teoria del bilanciamento con richiamo alla. *formula di Frank*, fatta propria dalla Cass. pen., Sez. Un. 18/09/2014 n. 38343, Espenhahn, ha ricondotto le fattispecie delittuose causate dalla violazione di regole cautelari, dapprima agevolmente riconducibili al dolo, nell'alveo della responsabilità colposa, la cui risposta sanzionatoria non era considerata adeguata al disvalore sociale di tale condotta.

[6] Il riferimento è alle alterazioni psicofisiche per assunzione di sostanze stupefacenti, ovvero per stato di ebrezza ovvero ancora per specifiche condotte che contravvengono le basilari disposizioni che regolano la circolazione stradale, quale la inversione del senso di marcia in prossimità di intersezioni, ovvero per chi raggiunge elevati spread di velocità rispetto ai limiti consentiti.

[7] Luparia, (2007a), p. 131.

c.d. *file* di *log*. Tale documento digitale può essere generato dal dispositivo (*log* di sistema), dalle singole applicazioni (di messaggistica istantanea ad esempio), ovvero anche dal *web* server.

Lasciando fuori dalla presente disamina le informazioni immagazzinate dai gestori di *server* o della rete, la cui acquisizione risulterebbe maggiormente problematica da vari punti di vista, non c'è dubbio che pare enorme la forza epistemica delle notizie archiviate *off-line* nel dispositivo del conducente del veicolo coinvolto nel sinistro: esse potrebbero assumere significativo peso nell'accertamento della responsabilità colposa di chi si trovava alla guida dell'autovettura la cui marcia ha determinato il decesso di una persona o altri gravi danni alla sua integrità psico-fisica. In effetti, i *data* di tali *file* se posti a sistema con altre evidenze processuali[8], quali le testimonianze, le informazioni ricavate da apparecchi elettronici installati sui veicoli (c.d. scatola nera), o, ancora, filmati delle registrazioni di videocamere installate nel luogo pubblico dello scontro, consentirebbero di accertare se l'evento lesivo sia eziologicamente ascrivibile alla violazione della disposizione di cui all'art. 173 co. 2 CdS.

2. Quali diritti e garanzie per lo *smartphone*?

Prima di concentrare l'attenzione sulla specifica valenza probatoria del *file* di *log*, è necessario vagliare il regime giuridico-processualistico dello *smartphone*, con riferimento alle informazioni in esso immagazzinate.

È innegabile che tale dispositivo abbia acquistato, nel corso degli ultimi anni, un peso fondamentale nella vita quotidiana, in quanto rappresenta il mezzo attraverso cui l'individuo estrinseca la propria personalità e alimenta la propria dimensione sociale e relazionale, gestendo costantemente i propri affari in modo ergonomico. Per tale ragione, l'ordinamento protegge, dietro la minaccia della sanzione penale, *id est* ai sensi dell'art. 615-ter c.p., i sistemi elettronici ed informatici da accessi abusivi.

Sorvolando la discussione in ordine alla natura del bene giuridico presidiato dalla norma incriminatrice, che solo apparentemente pare sovrapponibile alla discussione qui condotta, si deve chiarire quale tutela vada riconosciuta all'utilizzatore dello *smartphone*, ed ai dati in esso presenti, dinanzi all'attività investigativa dell'autorità finalizzata ad accertare se ve ne sia stato un utilizzo durante la marcia.

Ai fini di una analitica trattazione delle problematiche sottese a queste nuove entità, non pare peregrino distinguere una duplice dimensione dello *smartphone*, una di natura statica, immagazzinatrice di informazioni o *data*, ed una dinamica, in relazione alla sua idoneità di generare flussi di informazioni e comunicazioni. Se con riferimento al secondo aspetto, le compressioni della libertà e segretezza delle comunicazioni devono muoversi entro il perimetro di tutela delineato dall'art. 15 Cost, nello specifico della riserva di legge, della garanzia giudiziaria e del principio di motivazione, il discorso pare da impostare diversamente in relazione ai dati immagazzinati nel dispositivo, ivi compresi *sms*, le *e-mail* ovvero i messaggi inviati attraverso le applicazioni di dialogo istantaneo (*Whatsapp*, *Messanger* ecc) e memorizzati nel dispositivo ovvero nei *server* cui il dispositivo costituisce la porta di accesso. Tali dati, infatti, non rientrano nella categoria di intercettazioni delle comunicazioni, neppure nella declinazione informatica, e pertanto possono essere considerati come giacenti al di fuori dall'usbergo degli artt. 15 Cost. e 266 e ss. c.p.p.[9].

Deve essere quindi presa in considerazione un'ulteriore dimensione del dispositivo elettronico, quella correlata al suo essere contenitore di informazioni autoprodotte o semplicemente salvate e catalogate e, in relazione a tale dimensione, ci si deve interrogare, da un lato, su quali possano essere i presidi sulla cui base predicare la inviolabilità del dispositivo rispetto ad eventuali invasioni della Pubblica autorità per esigenze investigative; dall'altro, a quali condizioni la Pubblica autorità può superare tali presidi per appropriarsi delle preziose informazioni contenute nei cellulari di nuova generazione.

Tenuto conto del fondamentale rilievo che lo *smartphone* possiede nell'espletamento delle azioni quotidiane, configurando una articolazione spaziale, pur se non fisica, ove si proietta costantemente la sfera più intima della persona, si può affermare che quel luogo, pur se solo virtuale, possa assumere il valore di *domicilio* di cui all'art. 14 Cost. Sposando, dunque, un'in-

[8] Ha sostenuto la ridotta «autonomia dimostrativa» della prova digitale, L. Luparia, (2007b), p. 145.
[9] Cfr. Cass. pen., Sez. V., 21/11/2017, n. 1822.

terpretazione evolutiva, e non storica della disposizione costituzionale testé richiamata, il diritto fondamentale si estenderebbe anche all'involucro materiale, non limitandosi alla garanzia della riservatezza dei dati ivi contenuti[10].

Dando conto, invece, dell'impostazione più diffusa nel diritto vivente, sviluppatasi anche sull'approfondimento teorico della giurisprudenza costituzionale tedesca la quale ha riconosciuto il diritto alla segretezza ed integrità dell'informazione contenuta nel dispositivo informatica, quale declinazione evolutiva del diritto alla dignità personale[11], l'art. 2 Cost. si manifesta come norma generale che, nel tutelare la dignità fondamentale, presidia la c.d. riservatezza informatica la cui resistenza ad invasioni dell'autorità, per finalità investigative, si fonda sul carattere *contra legem*, nonché sproporzionato, dell'attività strumentale al perseguimento delle responsabilità penali. Tale attività di permeazione nello spazio digitale dell'individuo, prima compiuta con interpretazioni estensive dei mezzi di ricerca della prova tipizzati, ha riacquisito una nuova tipicità, specifica per il dominio 'informatico', in ragione dell'adozione della convenzione di Budapest sul *cybercrime* (l. 18 marzo 2008 n. 48).

3. L'incidente stradale: i primi rilievi e l'attenzione allo *smartphone*.

Puntando al cuore del tema oggetto di trattazione, va evidenziato che in caso di scontro tra veicoli cui conseguono esiti letali a beni primari, è pronto l'intervento degli agenti di pubblica sicurezza, al fine di ripristinare i flussi della circolazione, nonché a svolgere i rilievi di polizia giudiziaria, con lo scopo di raccogliere gli elementi utili prodromici all'accertamento delle eventuali responsabilità penali.

Nel cennato frangente, la constatazione che tali incidenti lesivi della integrità fisica, talora anche letali, siano stati causati dall'utilizzo dello *smartphone* alla guida ha imposto una riflessione in ordine alle attività da espletare nell'immediatezza dello scontro, al fine di far compenetrare nelle azioni investigative tanto l'interesse a non disperdere i dati salvati nel dispositivo, utili ai fini dell'accertamento, quanto la riduzione del rischio di arbitrarie apprensioni da parte della Polizia giudiziaria.

In tale direzione, plurali Procure della Repubblica sul territorio nazionale, come ad esempio quelle presso i Tribunali del Friuli Venezia Giulia, ovvero presso i Tribunali di Trento o Modena, hanno emanato direttive che regolano gli accertamenti da compiere nella *scena criminis*, strumentali a verificare se il sinistro sia riconducibile all'uso dello *smartphone* durante la guida.

In particolare, il documento elaborato dalla Procura presso il Tribunale trentino prescrive che solo in presenza di elementi di fatto da cui poter ricavare presumibilmente che l'incidente fosse ascrivibile ad una distrazione c.d. elettronica[12], è possibile procedere ad un visivo esame, *id est* ispezione, sullo *smartphone* o altro dispositivo rinvenuto nell'abitacolo[13].

La cennata direttiva specifica altresì che i rilievi, ai sensi dell'art. 354 co. 2 c.p.p.[14] devono essere espletati dall'ufficiale di polizia giudiziaria, e solo in casi eccezionali dagli agenti, secondo la previsione dell'art. 114 disp. att., previo avvertimento della facoltà di nomina del difensore (356 c.p.p.).

Tale primo accertamento è comunque subordinato al consenso del proprietario e si limita nell'esame del dispositivo (applicazioni in funzione, schermate attive) nonché alle condizioni esterne dell'apparecchio, le cui risultanze sono annotate nel contestuale processo verbale. Il mezzo di ricerca della prova 'tipico', pur se espletato secondo le cennate modalità, espone all'evidente rischio di alterare la genuinità del dato informatico, che presenta elevato tasso di vo-

[10] In questo senso, R. Borruso, (1994), p. 28: secondo cui il dispositivo informatico è organo del singolo individuato, poiché è il contenitore «di tutte le conoscenze, i ricordi, i segreti».
[11] Sul tema affrontato dalla Corte Costituzionale tedesca, si veda il commento di Flor, (2009), p. 695 s.
[12] Si provvede ad una esemplificazione degli stessi: l'apparecchio viene rinvenuto sul tappetino anteriore, ovvero vicino ai piedi del conducente; la presenza del dispositivo acceso o in funzione di vivavoce; lo *smartphone* presenta rotture della scocca.
[13] Si tratterebbe di indagine informatica «non occulta» in quanto espletata sotto la percezione del soggetto destinatario, secondo la classificazione operata da M. Daniele, (2017), p. 267.
[14] È evidente infatti che il Pubblico Ministero non abbia ancora assunto la direzione delle indagini in ragione del peculiare atteggiarsi di tale vicenda rilevante per il diritto penale

latilità[15] ed alterabilità[16]. Inoltre l'eventuale riscontro visivo circa lo stato di accensione ovvero la presenza di applicazioni attive conduce in ogni caso ad una conoscenza marginale, che può presentarsi irrilevante o comunque insufficiente[17]. Si verrebbe a contraddire la regola basilare dell'attività di rilievo investigativo sul dato informatico che necessita di una cautela particolare al fine di evitare le contaminazioni dall'esterno tali pregiudicare il valore della *digital evidence*[18].

Nell'ipotesi di esito negativo dell'esame visivo dello *smartphone* condotto come detto su consenso del titolare, il dispositivo verrà restituito al titolare, con precisa indicazione nel verbale.

Diversamente, ove si ravvisano elementi fattuali che possano far presumere l'utilizzo del telefono, prosegue la direttiva, il dispositivo deve essere sottoposto a sequestro ai sensi dell'art. 354 co. 2 c.p.p., nel rispetto della procedura di custodia (assicurare che il dispositivo non si spenga, nonché escludere l'accesso al sistema da remoto mediante l'attivazione della specifica funzione, c.d. modalità aereo, ovvero mediante la creazione di una schermatura di alluminio o di gabbia di faraday). Si prevede specificamente anche l'invito rivolto al proprietario dell'apparecchio a fornire il PIN, previa comunicazione che pur in caso di diniego si provvederà con l'accesso forzato ai contenuti ivi presenti, anche a costo di danneggiarli[19]; mentre per ciò che concerne le modalità di custodia, ove la misura cautelativa involga una pluralità dispositivi rinvenuti negli abitacoli, essi verranno inseriti in buste differenti.

4. Il sequestro dello *smartphone* e del *file* di *log*.

Come già annunciato, l'attività ispettiva della polizia giudiziaria sul dispositivo elettronico nell'immediatezza dell'incidente non pare la soluzione più efficace in punto di successo investigativo. In effetti, il reperimento di elementi per sostenere l'accusa per omicidio o lesioni colpose stradali potrebbe, in modo più utile, transitare per il vaglio del *file* di *log*. Tale *metadato* digitale racchiude le operazioni compiute dall'utente con l'apparecchio, secondo uno specifico ordine temporale, ed è autoprodotto dal dispositivo che provvede a conservalo. Come di evidente valutazione, il *file di log* del sistema o delle singole applicazioni rappresenta una prova documentale che soggiace all'art. 234 c.p.p. di cui è consentita l'acquisizione poiché rappresenta il fatto «*mediante un qualsiasi altro mezzo*».

In tale senso, l'apparecchio che ha generato l'informazione e che materialmente la ospita si presenta solo come fonte di prova, giacché, come detto, l'elemento di prova ha natura digitale, e corrisponde specificamente al relativo documento digitale.

In questo senso occorre valutare se e in che limiti il dispositivo può essere sottoposto a vincolo di indisponibilità, funzionale all'estrazione di quell'informazione rilevante per l'accertamento della responsabilità penale. Ciò che va precisato è che l'ablazione dello *smartphone* è funzionale al sequestro probatorio del documento digitale ivi contenuto, il c.d. *file* di *log*, la cui estrazione non potendo avvenire nella contestualità dell'azione, dovrà essere condotta in diversa sede. Ne consegue che la misura cautelare ablativa deve essere supportata da elementi di fatto che sorreggano la prospettazione dell'utilizzo dello *smartphone* durante la marcia.

La complessità e le peculiarità dei sistemi informatici dello *smartphone*, con architetture differenti rispetto agli apparecchi fissi, impongono altresì di meditare sulle tecniche di *forensics analysis* per estrarre le informazioni salvate nel dispositivo mobile, anche alla luce dei differenti sistemi operativi installati (*Android*; *iOS*)[20].

La misura cautelare del sequestro del dispositivo è teleologicamente orientata all'estrazione di una copia digitale del *file di log*, Il vincolo di indisponibilità sull'apparecchio fisico viene quindi meno, dopo l'estrazione del documento digitale, espletata in modo tale da assicurare l'originalità del dato nonché la possibilità di svolgere (ripetibili) valutazioni sullo stesso.

[15] Per via della *data persistance* che impone un accertamento comunque nell'immediatezza e non a distanza di tempo, pena la cancellazione o sovrascrittura dei dati

[16] Sulla peculiarità del dato informatico, che presenterebbe i caratteri dell'immaterialità e fragilità intrinseca, si veda Di Bitonto, (2008) p. 504.

[17] Ciò in quanto le applicazioni possono rimanere attive nel dispositivo per lungo tempo, pur senza che le stesse siano in uso.

[18] Così espressamente prevede l'art. 354 co. 2 c.p.p. come modificato per via dell'art. 9 co, 3 l. 48/2008 che ha dato attuazione alla Convenzione di Budapest del Consiglio d'Europa sul Crimine informatico.

[19] Su tale indicazione, si rinvengono ombre della violazione del diritto al silenzio.

[20] I dispositivi mobili sono operano attraverso le c.d. memorie NAND Flash per i quali non sarebbe possibile svolgere una copia *bit* a *bit*.

Ne consegue che il vincolo di indisponibilità sulla *res* fisica non essendo supportato da alcuna altra ragione, dovrà essere travolto. Ciò consente di assicurare la conformità al principio di proporzionalità del vincolo che illumina l'intera disciplina della ingerenza dell'autorità nell'ambito procedimento penale[21].

5. Attività investigativa informatica e tutela del contraddittorio.

La creazione della *bit stream image*, o comunque di un intervento similare atto a fotografare i contenuti del dispositivo mobile, richiede di interrogarsi in ordine alla garanzie procedimentali in tale sede. In effetti, la copia forense può essere generata mediante l'utilizzo di particolari *software* a disposizione degli organi inquirenti, che assicurano l'assoluta identità con i dati originali. Tale attività di copiatura non può comunque essere svolta nell'immediatezza dei rilievi in sede di incidente stradale, poiché è richiesta una particolare strumentazione e competenze settoriali per la sua creazione.

Con riferimento a questo tema, ancora discussa risulta essere la possibilità che la cennata operazione d'indagine, e cioè l'estrazione della copia dei dati contenuti del dispositivo, debba essere espletata alla stregua di un accertamento tecnico irripetibile.

La giurisprudenza ha affermato che tale intervento investigativo non implica alcuna attività valutativa di carattere tecnico-scientifico dell'organo inquirente, né risulta essere compromesso il valore della genuinità dell'informazione in ragione del fatto che il dato potrà essere oggetto di continue valutazioni, senza rischio di alterazione[22].

La ricostruzione sposata dalla giurisprudenza di legittimità è stata sottoposta a critica nella parte in cui, con disinvoltura, non riconosce la singolarità dell'azione investigativa su elementi informatici, per i quali il concetto di irripetibilità dovrebbe specificarsi, in questo settore, nel diverso significato di *volatilità* o *alterabilità* della *digital evidence*[23].

L'attività d'indagine attraverso cui si procede all'estrazione della *bit strem image* dovrebbe essere espletata in modo tale da assicurare la garanzia del diritto di difesa del soggetto sospettato del reato, secondo le modalità dell'accertamento tecnico irripetibile (art. 360 c.p.p.), atteso che le conoscenze tecniche necessarie per tale intervento non sono comuni e comunque, come detto, la caratteristica di alterabilità dei dati impone la necessaria cristallizzazione del dato probatorio, ancor prima della sede normale di formazione della prova, il dibattimento[24].

Seguendo l'indirizzo tracciato dalla giurisprudenza per cui l'estrazione di una copia forense deve essere effettuata unicamente nel rispetto delle *best practices* elaborate dalla *computer forensics*, si ricava che la garanzia dell'integrità della *bit stream image* rispetto al dato originale viene adeguatamente assicurata dalla etichetta generata dalla funzione di *hash*[25]. Particolare cura deve essere poi riservata anche alla conservazione della copia forense, così da scongiurare che sulla stessa intervengano alterazioni *medio tempore*, e comunque prima dell'espletamento delle analisi processuali sulla *digital evidence*[26].

6. L'equilibrio per il *file* di *log*.

Ai fini dell'accertamento della responsabilità dei reati di omicidio e lesioni colpose stradali, l'interesse finalizzato all'accertamento non investe tutti i dati informatici contenuti nel dispositivo, bensì può essere limitato solo a quei *file* che registrano le operazioni di dialogo tra l'utente e la macchina, da cui poter ricavare la specifica scansione temporale di tale uso nel

[21] In punto di sproporzione del vincolo reale, Cass. pen., Sez. VI, 24 febbraio 2015, n. 24617, in *Cass. pen.,* 1, 2016, p. 286.; in generale, si veda Caianello (2014) p. 143 s.; nonché, in chiave più specifica, Nicolicchia, (2018), p. 1 s.

[22] In questo senso, tra le prime pronunce, Cass. pen., Sez. I, 5 marzo 2009, n. 14511, Aversano Stabile, in Cass. pen., 4, 2010, p. 1520 e ss, con nota di Lorenzetto . Cass. pen., Sez. I, 9 marzo 2011, n. 17244, in Cass. pen., 2, 2012, p. 440 con commento critico di Daniele il quale evidenzia come è indimostrato che l'oggetto dell'indagine informatica non venga modificato a seguito dell'estrazione del dato digitale. Sulla stessa linea interpretativa, a seguire, Cass. pen., Sez. V, 16 novembre 2015, n. 11905, Branchi, *CED* 266477.

[23] Marafioti (2011), p. 4509 s., e spec. 4519.

[24] Lorenzetto (2009), p. 154 s.

[25] Si tratta di una particolare funzione crittografica che assicura la rispondenza della copia rispetto al dato digitale originale che si voleva duplicare.

[26] Si consenta il rinvio generale alla monografia di Signorato (2018) ove l'Autrice ha sistematizzato la materia delle indagini informatiche.

tempo antecedente l'incidente. Si tratta del c.d. *log*, meta-dato che automaticamente genera e raccoglie le informazioni relative al funzionamento del sistema, con il peculiare fine di consentire agli sviluppatori un riscontro dei problemi tecnici del sistema operativo o della singola applicazione.

Orbene, per l'accertamento di reati in esame, tale *digital evidence* può rappresentare un equilibrato compromesso tra l'interesse ad un efficace accertamento dell'utilizzo dello *smartphone* alla guida causativo di morte o lesioni personali – cui si correla la funzione di prevenzione generale nei confronti di un fenomeno dalla pervicace diffusione[27] – e le libertà fondamentali, in particolare la riservatezza e la libertà delle comunicazioni; quest'ultima viene in rilievo qualora il guidatore-utente stesse utilizzando programmi per lo scambio di messaggi.

In effetti, maggiore cautela deve essere poi assegnata ai *file* di *log* ovvero ai *file* di cronologia delle applicazioni di messaggistica istantanea, ad esempio *Whatsapp*. Seppur le informazioni di cui sopra costituiscono prova documentale e non intercettazione di flussi comunicativi nella modalità informatica[28], per ciò che concerne la specifica questione, e cioè se lo scontro tra veicoli sia ascrivibile all'utilizzo dello *smartphone* durante la marcia, l'interesse investigativo è limitato al solo dato esterno della conversazione, ulteriormente scremato: non è rilevante infatti conoscere il contenuto del messaggio né il destinatario/mittente, bensì l'attenzione deve concentrarsi solo sull'*an* ed il tempo in cui il guidatore abbia violato la regola cautelare distraendo la propria attenzione dal controllo dell'autovettura, così da ricostruire se vi è stata distrazione tecnologica in grado causare l'evento naturalistico (morte o lesioni gravi o gravissime)[29].

La conoscenza ricavabile dal *file* di *log*, in ogni caso, non è in grado di per sé di raggiungere esiti risolutivi; essa costituisce 'solo' una evidenza da considerare insieme ad altre, sia dichiarative sia documentali. Appare però una soluzione percorribile, giacché senza frustrare la finalità investigativa, assicura una proporzionata, e quindi legittima, invasione del diritto fondamentale al rispetto della vita privata (art. 8 CEDU)[30].

Bibliografia

Borruso Roberto (1994): "La tutela del documento e dei dati" in Borruso Roberto, Buonomo Giovanni, Corasaniti Giuseppe, D'Aietti Gianfranco, *Profili penali dell'informatica*, (Milano, Giuffrè), 1994, p. 28.

Caianello Michele (2014): Il principio di proporzionalità nel procedimento penale, in *Diritto penale contemporaneo – Rivista Trimestrale*, 3-4, p. 143 s.

Daniele, Marcello (2012): "*Il diritto al preavviso della difesa nelle indagini informatiche*", in *Cassazione penale*, 2, p. 441 s.

Daniele, Marcello (2017): "Le indagini informatiche contro il terrorismo", in Wein Roberto, Fornasari Gabriele (a cura di), *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, (Trento, Editoriale Scientifica), p. 267.

Daniele, Marcello (2018): "La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge", in *Processo penale e giustizia*, 5, p. 831 s.

Di Bitonto, Maria Lucia (2008): "L'accertamento investigativo delle indagini sui reati informatici", in *Diritto dell'internet*, 5, p. 504.

[27] La possibilità di ricostruire con certezza se lo scontro tra veicoli sia ascrivibile alla violazione dell'art. 173 co. 2 CdS porta con sé un'indubbia forza deterrente avverso tali distrazioni per la generalità dei consociati.
[28] Si rinvia a nt. 9.
[29] Si coglie in effetti la preoccupazione esternata in materia di indagini informatiche, pur se con peculiare riferimento alle forme di captazione dei dati *on-line* da M. Daniele, (2018), p. 831 s.
[30] Tra gli ultimi arresti in materia di limiti all'ingerenza arbitraria dell'autorità nella vita privata, con riferimento all'attività di perquisizione, Corte e.d.u. del 27/09/2018, Brazzi contro Italia, ric. n. 57278/11, § 41.

Flor Roberto (2009): "Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung", in *Rivista trimestrale di diritto penale dell'economia*, 3, p. 695.

Lorenzetto, Elisa (2010): *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in Cassazione penale, 4, p.

Lorenzetto Elisa (2009): "Le attività urgenti di investigazione informatica e telematica", in Luparia Luca (a cura di), Sistema penale e criminalità informatica (Milano, Giuffrè), p. 154 e ss.

Luparia, Luca (2007a): "Processo penale e scienza applicata", in Luparia Luca, Ziccardi Giovanni, *Investigazione penale e tecnologia informatica*, (Milano, Giuffrè), p. 131.

Luparia, Luca (2007b): "La ricerca della prova digitale", in Luparia Luca, Ziccardi Giovanni, *Investigazione penale e tecnologia informatica*, (Milano, Giuffrè), p. 145.

Mantovani, Ferrando (2015): "*Diritto Penale, Parte generale*", (Padova, CEDAM), p. 173.

Marafioti, Luca (2011): "*Digital evidence* e processo penale", in *Cassazione penale*, 12, 2011, p. 4509 s.

Nicolicchia Fabio (2018): "Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova", in *www.penalecontemporaneo.it*, 8/01/2018, p. 1 s.

Signorato, Silvia (2018): *Le indagini digitali. Profili strutturati di una metamorfosi investigativa* (Torino, Giappichelli).

Veneziani Paolo (2003): "*Regole cautelari "proprie" ed "improprie"*", (Padova, Cedam), p. 20 s.

Spunti per una riflessione sul rapporto fra biometria e processo penale*

Ideas para reflexionar sobre la relación entre biometría y proceso penal

Ideas for a Reflection on the Relationship Between Biometrics and Criminal Trial

Ernestina Sacchetto
Dottoranda di ricerca in "Diritti e Istituzioni" presso l'Università degli studi di Torino
ernestina.sacchetto@unito.it

Prova scientifica | Prueba pericial | Forensic evidence

Abstracts

Lo scritto si propone di offrire una panoramica dei caratteri principali della disciplina biometrica e di alcune problematiche emergenti dalla sua applicazione nel processo penale: a partire da necessarie precisazioni terminologiche si passerà all'esposizione del metodo biometrico corredato dalle relative misure di accuratezza che i vari sistemi di riconoscimento possono presentare in livelli differenti. Ci si prefiggerà altresì di illustrare le più diffuse tecnologie di identificazione e autenticazione tra cui le impronte digitali, il riconoscimento del volto, la misurazione dell'iride e della retina, la voce, l'andatura e la prova genetica. Tali sistemi biometrici presentano sicuri vantaggi applicativi non solo in ambiti privati (dall'accesso a determinati luoghi al godimento di vari servizi) ma anche nell'ambito processuale penale, in termini investigativi e probatori. Dopo aver fatto cenno allo "stato dell'arte" della prova scientifica, si focalizzerà l'attenzione su alcune possibili criticità emergenti dal rapporto fra la scienza biometrica e il processo penale. In primis, si rileva una confusione terminologica, dettata dall'assenza di una definizione unica, tanto in letteratura quanto in giurisprudenza, dell'aggettivo "biometrico". In secondo luogo, ad oggi non vi sarebbero ancora risultati univoci in termini di affidabilità di tali tecniche di riconoscimento e una riflessione complessiva va avviata con riguardo alla compatibilità con i principi costituzionali e le garanzie processuali.

El presente artículo tiene por finalidad ofrecer un panorama de las principales características de la disciplina biometría y de algunos problemas emergentes respecto a su aplicación en el proceso penal. Luego de algunas necesarias precisiones terminológicas, se expone en general el método biométrico, describiendo las principales tecnológicas de identificación y autentificación, entre las cuales se encuentra la huella digital, el reconocimiento facial, la medida del iris y retina, el reconocimiento de voz y la prueba genética. Estos sistemas biométricos presentan ventajas no solo en el ámbito privado, sino que también en el contexto del proceso penal, en términos investigativos y probatorios. Después de describir el "estado del arte" de la prueba científica, el trabajo se concentra en algunos posibles problemas relativos a la relación entre la ciencia biométrica y el proceso penal. En primer lugar, se evidencia una confusión terminológica, dictada por la ausencia de una definición única, tanto en la literatura como en la jurisprudencia, del adjetivo "biométrico". En segundo lugar, hasta la fecha todavía no existen

* I miei più sentiti ringraziamenti vanno agli organizzatori del nono corso di formazione interdottorale di Diritto e Procedura Penale "Giuliano Vassalli" per Dottorandi e Dottori di ricerca (Siracusa International Institute in collaborazione con il gruppo italiano dell'Associazione Internazionale di Diritto Penale - AIDP) intitolato "Nuove frontiere tecnologiche e sistema penale - Sicurezza informatica, strumenti di repressione e tecniche di prevenzione" nonché ai tutores del mio progetto di ricerca, il Professor Francesco Caprioli e la Professoressa Barbara Lavarini. Alla Prof.ssa Serena Quattrocolo va la mia profonda riconoscenza per il Suo contributo alle riflessioni confluite nel presente lavoro.

resultados inequívocos en términos de la confiabilidad de estas técnicas de reconocimiento, siendo necesaria una reflexión general respecto a su compatibilidad con los principios constitucionales y las garantías procesales.

The paper aims to offer an overview of the main features of the biometric discipline and of some problems, emerging from its application in the criminal trial: starting from the necessary terminological clarifications, the biometric method will be presented taking into account the relative accuracy measures that the various systems of recognition may offer in different levels. It will also aim to illustrate the most widespread identification and authentication technologies, including fingerprints, face recognition, iris and retina measurement, voice, gait and genetic testing. Such biometric systems have certain practical advantages not only in private areas (from access to specific places to the use of various services) but also in the criminal trial, in terms of investigations and evidence. After describing the "state of the art" of scientific evidence, particular attention will be devoted to some potentially critical issues, emerging from the relationship between biometric science and the criminal trial. First of all, there is a terminological confusion, deriving from the lack of a single definition, both in literature and in the case-law, of the adjective "biometric". Secondly, to date there are still no unambiguous results in terms of reliability of such recognition techniques and an overall reflection should be started with regard to compatibility with constitutional principles and procedural safeguards.

Sommario

1. Delimitazione del campo d'indagine.

Prima di avviare un'analisi intorno ad alcune questioni connesse all'applicazione della scienza biometrica nel processo penale, si ritiene fondamentale delimitare il campo d'indagine attraverso, in primo luogo, una chiara comprensione del significato del termine "biometria". Tale inquadramento non è facilmente realizzabile, essendo il campo della scienza biometrica assai variegato e complesso[1].

1.1. *Biometria. Precisazioni terminologiche.*

La biometria (dal greco *βίος*=vita e *μέτρον*= misura) è la disciplina che studia le grandezze biofisiche, sia fisiologiche sia comportamentali, allo scopo di identificarne i meccanismi di funzionamento, di misurarne il valore e di indurre un comportamento desiderato in specifici sistemi tecnologici[2]. Si tratta, dunque, della scienza avente ad oggetto la misurazione delle caratteristiche biologiche tipiche degli organismi viventi, attraverso l'applicazione di alcune tecniche specifiche[3]. Da un punto di vista tassonomico, in letteratura, con il termine "biometria", si è soliti riferirsi tanto al dato biologico grezzo proveniente da un determinato soggetto, quanto ai particolari sistemi tecnologici che permettono l'identificazione, l'autenticazione o la verifica automatica dell'identità, specie in luoghi o ambiti ove si pongono concrete esigenze di garanzia legate alla sicurezza pubblica o privata[4]. Per tale ragione, non sempre risulta facile, per chi si approccia allo studio di tale materia, comprenderne la sistematica e la regolamentazione nei vari ordinamenti.

Le caratteristiche biometriche oggetto di misurazione sono generalmente dotate di alcune proprietà essenziali ai fini identificativi e autenticativi tra cui l' "universalità" - il tratto deve essere comune nella popolazione - e l' "unicità", ossia l'elemento in esame deve avere un'alta riferibilità individualizzante[5].

La prima distinzione da compiere è quella tra caratteristiche biometriche anatomiche o fisiologiche, basate su dati derivanti da misurazioni effettuate su caratteristiche fisiche di una persona, quali l'impronta digitale, l'iride, la retina, la geometria della mano, i tratti somatici del volto[6] e caratteristiche biometriche comportamentali basate su dati che riguardano aspetti riconducibili a comportamenti propri di un determinato soggetto, quali il riconoscimento vocale, la dinamica di apposizione della firma, l'andatura ecc..

I principali obiettivi che la scienza biometrica si pone, dunque, sono due: in *primis*, verificare la dichiarazione di identità della persona e in secondo luogo, associare l'identità a un

[1] Amato *et. al.* (2013), p. 10.
[2] Cfr. "Biometria", Enciclopedie on line - Istituto dell'Enciclopedia italiana Treccani, http://www.treccani.it/enciclopedia/biometria/ (ultima visualizzazione il 19/2/2019).
[3] Cfr. Preite (2016), p. 21.
[4] Cfr. Presidenza del Consiglio dei Ministri - Comitato Nazionale per la Bioetica (2010), p. 10, *http://bioetica.governo.it/media/1846/p95_2010_identificazione-corpo-umano-biometria_it.pdf* (ultima visualizzazione il 18/2/2019).
[5] Altri parametri che generalmente si valutano sono: 1) *invarianza*: la caratteristica deve mantenersi costante nel tempo e indipendente rispetto a qualsiasi variabile; 2) *ammissibilità*: la misurazione deve rispettare l'integrità fisica della persona per poter essere condotta senza metodi troppo invasivi; 3) *acquisibilità*: qualità che consente la rilevazione in modo breve e semplice; 4) *affidabilità*: tale peculiarità deve permettere la ripetizione delle operazioni per verificarne l'esito; 5) *privacy*: riguarda la possibilità di adottare accorgimenti idonei al rispetto della riservatezza; 6) *riducibilità*: consiste nella possibilità di organizzare i risultati e renderli disponibili nelle successive consultazioni; 7) *grado di gradimento*: indica il livello con il quale ogni individuo accetta la metodologia biometrica applicata. Per un approfondimento sul tema tra gli altri cfr. Terraciano (2014), pp. 238-239 e Wayman *et al.* (2005), p. 2.
[6] Preite (2007), p. 43.

soggetto. In caso di accesso "fisico", il controllo biometrico si realizza attraverso una procedura di accertamento della titolarità personale all'ingresso di una zona o un'area riservata, un edificio protetto, ecc. In caso, invece, di accesso "logico", il controllo biometrico è effettuato tramite una procedura di accertamento circa la legittimazione della persona interessata (utente) a usufruire di una determinata risorsa informatica. A tal proposito, giova riportare la distinzione fra "verifica", in cui i dati acquisiti in un determinato momento dal sensore biometrico sono comparati con un unico dato depositato dall'utente nella fase di registrazione e custodito su un dispositivo sicuro o in un archivio magnetico indicizzato (per es. un codice identificativo), e "identificazione", in cui i dati acquisiti in un determinato momento dal sensore biometrico sono comparati con un insieme di dati contenuti in un archivio o *database*. Pertanto, autenticare significa confrontare un campione biometrico presentato con il corrispondente dato biometrico registrato, relativo ad una singola persona[7], per accertare che il soggetto sia realmente chi dichiara di essere. I sistemi biometrici di autenticazione/verifica accertano la corrispondenza univoca, effettuando un raffronto di tipo "uno contro uno" tra specifiche caratteristiche fisiche o comportamentali di un individuo stesso, registrato in un *database* o in un dispositivo mobile[8]. L'identificazione è, invece, un vero e proprio processo di attribuzione dell'identità, che si realizza attraverso il raffronto dei dati biometrici di un individuo con tutti quelli memorizzati in un *database*, effettuando un confronto "uno contro molti". Un sistema può compiere un'identificazione positiva o negativa, dichiarando l'individuo rispettivamente di appartenere o non appartenere al gruppo di utenti noti al sistema.

Nel contesto attuale, i campi di applicazione di tale disciplina risultano i più svariati: dall'accesso a determinati luoghi, al godimento di particolari servizi, alla tracciabilità, con un'evoluzione tecnologica nei campi più differenti (tutela della salute, prevenzione delle frodi sanitarie, protezione dei dati riservati, monitoraggio dell'accesso ad aree riservate, efficienza in attività commerciali, sicurezza nel campo finanziario e militare, controllo alle frontiere e dei flussi migratori etc.)[9]. Il dato proveniente da una precedente autenticazione potrebbe rivelarsi altresì rilevante dal punto di vista penale, per l'accertamento di qualunque elemento utile in ambito investigativo ma anche probatorio[10], eventualmente pure al fine del giudizio di responsabilità.

1.2. *L'*iter *biometrico: dal dato biologico grezzo al* template"

Il metodo di riconoscimento biometrico comincia con la fase di registrazione (*enrollment*), ossia con la rilevazione e l'acquisizione della caratteristica biometrica sotto forma di "dato biometrico grezzo" da parte del sensore cui segue la conversione in un *template*[11]. Quest'ultimo, detto anche "modello biometrico", costituisce una rappresentazione matematica digitale del campione biologico. I sistemi di identificazione biometrici archiviano e confrontano per lo più *templates* e non dati biometrici grezzi, i quali vengono principalmente utilizzati per la creazione del *template*.

Una volta terminata la fase di *enrollment*, si apre la procedura di comparazione dei *templa-*

[7] Council of Europe, *Consultative commitee of the convention for the protection of individuals with regard to automatic processing of personal data*, *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, p. 8, «*Verification means comparing a presented biometric sample with the corresponding enrolled biometric data pertaining to one single person*», https://rm.coe.int/16806840ba (ultima visualizzazione il 19/2/2019).

[8] Bisi (2005), pp. 3-35.

[9] Presidenza del Consiglio dei Ministri - Comitato Nazionale per la Bioetica (2010), pp. 4-5, *http://bioetica.governo.it/media/1846/p95_2010_identificazione-corpo-umano-biometria_it.pdf* (ultima visualizzazione il 18/2/2019).

[10] «Si pensi all'impiego processuale del DNA rinvenuto sul corpo della vittima, quale indizio a carico dell'imputato; al riconoscimento come autentico o meno di un testamento olografo, sulla base dei tratti caratterizzanti la grafia del testatore; alla presenza sulla mano dell'imputato, accusato di aver ucciso taluno con un'arma da fuoco, di tracce di polvere da sparo; alle analisi cliniche e tossicologiche utilizzate per accertare lo stato di salute o le condizioni fisiche dell'imputato o della vittima; alle metodiche di riconoscimento della voce umana in base alla biometria; alle tecniche di pedinamento satellitare; e via discorrendo». Giunta (2014), p. 565. Per un approfondimento di veda tra gli altri anche Tistarelli e Champod (2017), pp. 5 e ss..

[11] Nanavati *et al*. (2002), p. 17. Si ritiene opportuno specificare che il concetto di *template*, così come quello di campione biologico grezzo risulta centrale per la comprensione e l'analisi delle problematiche relative alla riservatezza piuttosto che alla compatibilità fra le varie tecnologie biometriche e i principi costituzionali posti a garanzia dell'individuo. Infatti, a seconda che il dato venga memorizzato nell'una o nell'altra forma, potrebbe richiedersi una tutela differente, più o meno rafforzata.

tes[12], per determinare il loro grado di somiglianza e di correlazione[13]. Il confronto viene attuato fra il *template* archiviato mediante il processo di *enrollment* (*enrollment template*), e il *template* creato quando l'utente fornisce il proprio dato biometrico al dispositivo di rilevazione del dato stesso (*verification template*). Al livello di somiglianza viene solitamente assegnata una votazione che, in quasi tutti i sistemi, è valutato rispetto a un numero predefinito che funge da limite minimo[14]. Se il punteggio eccede la soglia, si verificherà il cd. *match* (combinazione dei *template*) e l'individuo sarà riconosciuto, nel caso opposto la coincidenza non avverrà e il riconoscimento fallirà (*non match*)[15]. Dal momento che ogni *template* è unico, le due stringhe di dati, quella archiviata e quella ottenuta "in tempo reale", saranno diverse[16]. Per tale ragione, il sensore di cattura deve essere governato da uno specifico algoritmo, il quale consente di confrontare i differenti modelli biometrici per verificarne il grado di coincidenza, che in ogni caso non potrà mai essere totale, e determinare se esso ricade, in base alla valutazione attribuita, al di sopra o al di sotto della soglia considerata accettabile[17]. Pertanto, considerato che non è possibile raggiungere un grado di correlazione e somiglianza totale tra i *templates* confrontati, evidentemente la risposta che il sistema biometrico può fornire ai fini del riconoscimento di un soggetto non può che essere, in un certo senso, approssimativa[18].

1.3. *Tecniche di identificazione biometrica*

Il modo migliore per comprendere la portata applicativa della scienza biometrica nel processo penale, ponendo in luce gli aspetti più problematici, è analizzare, seppur per brevi cenni, alcuni dei sistemi d'identificazione più diffusi[19].

1.3.1. *Le impronte digitali*

L'identificazione basata sulle impronte digitali è da considerarsi una delle tecniche maggiormente utilizzate in biometria forense[20]. Tale sistema sfrutta in modo particolare le tracce

[12] Detta "*matching*".
[13] Navanati et al. (2002), p. 20.
[14] Tale valore minimo viene generalmente stabilito dall'amministratore del sistema cosicché, a seconda del grado di sicurezza desiderato, è possibile optare per sistemi con soglie più o meno elevate.
[15] È poco probabile che due campioni della stessa caratteristica biometrica, acquisiti in diverse sessioni, coincidano perfettamente (*ut infra*, nota n. 18): questo può verificarsi per molteplici cause, come la presenza di un "rumore", cambiamenti ambientali e la cattiva interazione con l'interfaccia, ossia la superficie del dispositivo attraverso la quale il dato biofisico è acquisito. L'*output* di un sistema di riconoscimento biometrico costituisce un risultato *s* che quantifica la somiglianza fra l'*input* e il *template* archiviato in precedenza nel *database*. Più si rivela elevato il valore del risultato *s*, maggiore sarà la possibilità che i due campioni coincidano. Le principali misure dell'accuratezza di un sistema biometrico sono FNMR, *False Non-Match Rate* e FMR, *False Match Rate*: 1) FNMR si riferisce alla probabilità che due campioni coincidenti, ossia campioni dello stesso tratto biometrico acquisiti dallo stesso utente, siano dichiarati erroneamente come provenienti da due diversi individui (la percentuale si trova anche indicata con la dicitura FRR ossia *False Rejection Rate*); 2) FMR è la probabilità attesa che due campioni appartenenti a due individui diversi siano erroneamente riconosciuti come coincidenti (oppure FAR ossia *False Acceptance Rate*); 3) infine, il parametro FTE (*failure to enroll*) indica la probabilità che un soggetto non sia in grado di essere registrato in un sistema biometrico (altri due parametri, utili ai fini di una comparazione globale dei sistemi, sono EER ossia l'*equal error rate*, che indica il tasso di errore nel punto in cui le curve FAR e FRR si incrociano, e l'*ability to verify* o ATV, che è una combinazione di FTE e FNMR, e indica la percentuale di utenti che saranno in grado di utilizzare il sistema su base giornaliera). La maggior parte dei *False Non-Match Rate* è dovuta a una cattiva interazione dell'utente col sensore del sistema e può essere facilmente risolta permettendo al soggetto di presentare nuovamente l'*input*. L'ipotesi di *False Match Rate*, invece, si riferisce ai tentativi di determinati soggetti che pur non essendone autorizzati, ottengono l'accesso a un sistema, portando a compimento attacchi alla sicurezza dello stesso. Si evince chiaramente che la ricerca del valore di soglia ottimale che permetta un efficace equilibrio fra FMR, FNMR e FTE, rappresenta una delle difficoltà maggiori che incontrano i gestori di sistemi di autenticazione e identificazione basati sulle tecnologie biometriche. Cfr. Delac e Grgic (2004), p. 10 e Jain *et al.* (2011), p. 328.
[16] Ogni *template* risulta unico e irripetibile in quanto, durante la fase di *enrollment* (*ut supra*, § 1.2), potrebbe subentrare la presenza di numerosi fattori contingenti che variano di importanza a seconda del tipo di dispositivo di rilevazione, come l'illuminazione ambientale, i rumori di sottofondo, il corretto posizionamento dell'utente, il livello di umidità e di temperatura etc.
[17] I sistemi d'identificazione o autenticazione biometrica utilizzano algoritmi proprietari per analizzare i *templates* e generare punteggi. Tali algoritmi trattano i dati contenuti nel *template*, al fine di effettuare un efficace confronto che tenga conto dei fatto di cui in nota n. 14. CNIPA, *Linee guida per l'impiego delle tecnologie biometriche nelle pubbliche amministrazioni. Indicazioni operative*, pp.25 e ss., http://www.ordineavvocatitrani.it/upload/linee_guida_tecnologie_biometriche.pdf (ultima visualizzazione il 19/2/2019).
Si veda come esempio di applicazione di quanto detto sopra Cass. pen. Sez. II, (ud. 11-11-2005) 05-12-2005, n. 44358.
[18] Per un approfondimento in materia si veda Iovane (2008), pp. 181 e ss.
[19] Di seguito si riporteranno le tecniche di riconoscimento biometrico più diffuse tralasciando quelle meno utilizzate o poco sfruttate nel contesto forense.
[20] Cassazione penale sez. II, 10/10/2018, (ud. 10/10/2018, dep. 25/01/2019), n.3654.

lasciate dalle piccole creste presenti sulle punte delle dita. Ad oggi, attraverso l'utilizzo delle apparecchiature digitali le impronte vengono estratte per mezzo di sensori[21]. Attraverso il metodo cd. *scanning* è possibile realizzare un'immediata registrazione dell'impronta digitale. Ancora più efficiente risulta la cd. "scannerizzazione in diretta", per la quale è anche possibile individuare valori specifici come la temperatura e le pulsazioni del cuore dell'individuo che viene sottoposto all'identificazione. Gli apparecchi digitali consentono, inoltre, di diminuire notevolmente le problematiche connesse alla scarsa definizione dell'immagine dell'impronta (per es. il calore e il sebo epidermico emanato dalle dita della mano). Il sistema di comparazione tra il campione estratto e quello digitale, ottenuto per essere conservato nei *database*, costituisce il principale punto di forza e, contestualmente, la problematica più complessa: i vantaggi si manifestano in termini di accuratezza, velocità e disponibilità immediata di dati ma, da un lato, emergono alcune difficoltà – seppur ad oggi parzialmente superate grazie al progresso scientifico-tecnologico – legate alla necessità che le apparecchiature dispongano di notevoli capacità di calcolo, dall'altro si segnalano le già accennate criticità legate ai falsi positivi[22].

1.3.2. *La geometria della mano*

Il sistema di riconoscimento della geometria della mano misura le caratteristiche fisico-geometriche della mano: la forma, la larghezza, la lunghezza delle dita e delle nocche e lo spessore del palmo (o dita). La principale tecnologia impiega una telecamera per catturare alcune misure geometriche comprensive di lunghezze, distanze ed angoli. Nonostante tale sistema, comparso sul mercato intorno agli anni Settanta del secolo scorso[23], sia utilizzato ormai da diversi anni, è ancora piuttosto dibattuto l'aspetto dell'unicità della geometria della mano. Alcuni studiosi sostengono che la geometria della mano non presenti elementi univoci tali da permettere di identificare un individuo come le impronte digitali. Anche dal punto di vista del parametro dell'*invarianza*[24], è oggetto di discussione fra gli esperti, poiché possono essere molteplici i cambiamenti nel tempo (per es. per l'età o malattie). Per tale ragione, il sistema considerato viene utilizzato soprattutto per le autenticazioni ossia in modalità "verifica" (cfr. *supra*, § 1.1)[25].

1.3.3. *Il riconoscimento facciale*

Il riconoscimento del volto è un sistema innato, utilizzato dagli esseri umani per riconoscersi gli uni con gli altri[26]. Il sistema biometrico basato sul riconoscimento del viso consiste in un metodo automatico o semi-automatico che registra e paragona le differenze della struttura geometrica del viso, tra cui la forma e la posizione dei suoi attributi – gli occhi, le labbra, il mento – e le loro relazioni spaziali. Durante la rilevazione del dato grezzo, un sensore registra un'immagine o una serie di immagini del volto del soggetto che vengono convertite in formato digitale. Un modello rileva le caratteristiche rilevanti e crea un *template* di dimensioni inferiori rispetto al volto originale rendendo possibile la sua memorizzazione su una *smartcard* o su un passaporto[27], utilizzati per i procedimenti di verifica d'identità. Gli strumenti biometrici basati sul riconoscimento facciale sono molto efficienti in quanto sono facilmente "collezionabili" e

[21] In tempi più risalenti, le impronte venivano estratte premendo la punta di un dito bagnata di inchiostro su di un semplice foglio di carta, in modo tale da lasciare traccia permanente al fine di effettuare gli studi e le comparazioni necessarie.
[22] Cfr. *supra*, nota n. 17. Le apparecchiature basate sull'identificazione delle impronte digitali sfruttano due elementi peculiari: le caratteristiche di dettaglio (*local ridges and furrow details* ossia l'analisi dettagliata delle creste e dei solchi dell'impronta digitale) e la configurazione globale (*global pattern configuration*, intesa come la configurazione dell'immagine globale dell'impronta). Relativamente allo studio dei dati raccolti, si è soliti distinguere fra l'approccio statistico (in cui si analizzano i dati oggettivi direttamente dai campi di immagine dell'impronta) e l'approccio strutturale (in cui invece si preferisce analizzare alcuni campioni rilevanti comparando fra loro le specificità). Recentemente, si è individuata una classificazione in riferimento agli algoritmi prima illustrati suddivisa in cinque categorie: arco, arco a tenda, cerchio sinistro, cerchio destro e spirale. Tali elementi vengono ottenuti attraverso la scansione digitale delle impronte, in seguito elaborate, seguendo le peculiarità generali e particolari, per poi analizzarli ai fini di ricerca statistica nei *database*, oppure compararli sulla base della loro struttura.
[23] Amato *et. al.* (2013), p. 31.
[24] Cfr. *supra*, nota n. 6.
[25] Yoruk et *al.* (2006), pp. 1083-1815.
[26] Amato *et. al.* (2013), p. 33.
[27] Tra i 100 e i 3500 byte per i *templates* e tra i 20-40 *kilobytes* per l'immagine originale.

capaci di catturare l'immagine a distanza senza che il soggetto possa accorgersene. Tuttavia, vi sono dei limiti nel sistema: le caratteristiche del volto sono soggette a dei mutamenti (per il trascorrere del tempo, per lesioni, per effetto della chirurgia estetica). La *performance* del sistema può essere influenzata da diversi fattori, quali la distanza del sensore, la visibilità del volto, il grado di cooperazione del soggetto e la qualità delle immagini[28].

1.3.4. *Il riconoscimento dell'iride e della retina*

I sistemi biometrici basati sulla struttura dell'iride sono in grado di identificare, in tempo reale, l'individuo attraverso la misurazione dell'iride[29]. Il soggetto guarda verso il sensore permettendo l'illuminazione della struttura dell'iride da parte di un laser a bassa intensità, una luce infrarossa che effettua la scansione dell'occhio e consente di rilevare le sue particolarità. Un algoritmo rappresenta in termini matematici la struttura dell'iride. I limiti dei sistemi di identificazione basati sul riconoscimento dell'iride sono legati al fatto che è necessario posizionare opportunamente l'occhio: il processo di localizzazione costituisce un importante passaggio, poiché, se eseguito scorrettamente, può comportare una contaminazione da parte di eventuali disturbi esterni in corso di riconoscimento (per es. i riflessi), oppure nei pressi dello stesso bulbo oculare (quali le ciglia e le pupille). Dal punto di vista del parametro dell'-"invarianza"[30], l'iride – a parte i primi mesi di vita – rimane pressoché immutata durante il corso della vita dell'individuo. Tale tecnica viene utilizzata soprattutto nell'ambito della sicurezza e non è considerata invasiva poiché non vi è alcun contatto fisico fra il soggetto e lo strumento di rilevazione.

Considerando, invece, il riconoscimento biometrico della retina (ad oggi, tecnica molto poco utilizzata), il principale aspetto caratterizzante è costituito dallo studio del sistema vascolare. Sebbene tale tecnologia venga considerata un'efficiente sistema di identificazione personale, essa risulta di difficile impiego e piuttosto invasiva[31].

1.3.5. *Identificazione basata su tratti "dinamici": il riconoscimento vocale e il modo di camminare.*

I sistemi biometrici basati sul riconoscimento vocale funzionano attraverso la misurazione della voce, componente comportamentale dell'individuo risultante dalle caratteristiche fisiche specifiche di ciascun individuo come la forma e la grandezza dei tratti vocali, del mento, delle cavità nasali, delle labbra[32]. Tali sistemi di identificazione sono utilizzati anche per i processi di verifica/autenticazione e hanno avuto recente diffusione in settori come la finanza (*e-commerce* e *e-banking*) e nell'ambito forense (la polizia giudiziaria registra la voce per poi eseguire il *matching* con la conversazione telefonica intercettata ai fini dell'indagine e se il confronto dà esito positivo, quest'ultimo può essere successivamente utilizzato come prova durante il processo[33]). La voce è da sempre considerata un parametro universale con un certo grado di "permanenza" (può modificarsi a seconda dell'età, dello stato emotivo o dello stato di salute) ed è di facile "collezionabilità"[34].

Per quanto concerne i sistemi biometrici basati sull'andatura del soggetto, essi funzionano a partire da una telecamera che cattura la specifica modalità in cui un soggetto cammina mi-

[28] Per un approfondimento si veda Mastronardi (2014), pp. 1-12; Cassazione penale sez. I, 03/12/2018, (ud. 03/12/2018, dep. 14/01/2019), n.1524.
[29] Amato *et al.* (2013) p. 35. Per un approfondimento sul tema si veda anche La Regina (2018), p. 212.
[30] Cfr. *supra*, nota n. 6.
[31] La tecnica necessita di un contatto fra il sensore e l'occhio del soggetto: nella maggior parte dei casi, tale sistema di identificazione è percepito dagli utenti come pericoloso.
[32] Cfr. Grimaldi *et al.* (2014), p. 2014. Le tecnologie legate a tale dato biometrico possono essere di due tipologie: il *text dipendent* e il *text indipendent*. Nel primo, il soggetto da identificare pronuncia una frase che, tradotta in *template*, viene codificata in un algoritmo. Nel secondo, la voce del soggetto è riconosciuta a prescindere da ciò che sta proferendo: le onde sonore emesse dall'individuo sono registrate e calcolate come vettori caratteristici che vengono assunti da modello (*template*) dell'individuo. Durante la fase di riconoscimento, le sequenze dei vettori vengono comparate usando il campione.
[33] Amato *et al.* (2013), p. 37.
[34] Cfr. *supra*, nota n. 6.

surando la forma e/o le dinamiche del corpo, l'andatura delle gambe, la cadenza e la velocità del passo[35]. L'andatura non è considerata una caratteristica "universale" ma è comunque un elemento identificativo. Dal punto di vista della "permanenza", esso può variare a seconda della muscolatura, con il trascorrere del tempo, durante la gravidanza, a causa di lesioni o in condizioni alterate dell'individuo (per es. in stato d'ebbrezza).

1.3.6. *L'analisi del DNA.*

Ciascun essere umano è identificabile attraverso il proprio codice genetico del DNA: esso si può definire come una lunga molecola presente all'interno delle nostre cellule, nella quale si raccoglie un enorme quantità di informazioni necessarie per lo sviluppo dell'individuo, per la costruzione di ampie varietà di strutture biologiche e per il mantenimento dei processi vitali[36]. Alla base del lavoro dei genetisti forensi vi è l'acquisizione delle sezioni di tali molecole al fine di descriverne le singole caratteristiche genotipiche[37].

La profilazione del DNA in ambito forense è ormai un mezzo di prova generalmente accettato da parte delle autorità giurisdizionali, tanto da aver portato alla costituzione di *database* specifici in un'ottica di cooperazione internazionale, per fini legati all'identificazione personale e alla sicurezza.

Tutte le cellule dotate di un nucleo contengono frammenti di DNA identico per un medesimo individuo e perciò la maggior parte dei materiali biologici lasciati dal nostro corpo consentono di risalire all'identità personale[38]. Solitamente in ambito forense vengono comparati due profili di DNA: uno rilevato sul luogo del delitto ed un altro di riferimento, estratto da un sospetto criminale. Nessun problema si pone se i due profili risultano essere differenti mentre, se i due profili corrispondono, allora sarà necessario comprendere se il campione di DNA ricavato dalla *scena criminis* appartiene realmente al sospettato o a qualcun altro avente lo stesso profilo genetico (la probabilità che ciò si verifichi è pari a 1 su un miliardo)[39]. Vi sono poi numerosi altri fattori che possono elevare la possibilità che si tratti di un errore di falsa corrispondenza: il campione biologico grezzo potrebbe contenere solo una minima quantità di DNA o il profilo rilevato sul luogo del delitto potrebbe essere stato danneggiato o contaminato. L'evoluzione tecnologica e digitale ha consentito un notevole miglioramento degli studi scientifici e delle tecniche di analisi dei campioni di DNA e il diritto ha tentato negli anni di disciplinare l'utilizzo di tali tecniche[40].

2. La cornice normativo-giurisprudenziale della prova scientifica: le linee di fondo in materia.

Con l'espressione "prova scientifica" s'intende correntemente qualsivoglia accertamento che produca un risultato utile per il processo e che richieda per il suo espletamento il ricorso

[35] Alla base del funzionamento di tale tecnica vi è l'utilizzo di un algoritmo per la determinazione delle relazioni matematiche intercorrenti fra ogni punto del corpo in movimento ed il *template* necessario al fine del riconoscimento. Si veda Ass. App., Torino, n. 21/15 Reg. Sent., 22.02.2016; Cassazione penale sez. I, 03/12/2018, (ud. 03/12/2018, dep. 14/01/2019), n.1524; Cassazione penale sez. I, 08/06/2018, (ud. 08/06/2018, dep. 13/09/2018), n. 40722.

[36] L'analisi del DNA è stata recentemente ammessa tra le tecnologie biometriche che sono all'attenzione del sub-comitato di standardizzazione ISO (ISO/IEC JTC1 SC 37 "*Biometrics*") anche se, a differenza di quanto avviene per tutte le altre tecnologie biometriche, almeno per il momento l'analisi del DNA non permette un'autenticazione in tempo reale. Quest'ultimo criterio non è tuttavia contemplato nella canonica definizione di tecnologie biometriche e quindi non impedisce di annoverare l'analisi del DNA tra di esse.

[37] In tempi più risalenti veniva utilizzato il metodo *fingerprint*, in cui il profilo genetico era raffigurato con una sezione di grafico a barre. Successivamente, grazie al metodo *Mullis* e la cd. "reazione a catena della polimerasi", il profilo genetico veniva descritto con una semplice sequenza di numeri: il frammento del DNA studiato viene riprodotto diversi milioni di volte, in modo da poterlo analizzare a livello macroscopico. Cfr. "*Fingerprinting*", Enciclopedie on line - Istituto dell'Enciclopedia italiana Treccani, http://www.treccani.it/enciclopedia/fingerprinting_(Dizionario-di-Medicina)/ (ultima visualizzazione 19/2/2019).

[38] Dal punto di vista della preparazione dei campioni e delle modalità di analisi, si ritiene come i marcatori del DNA siano collocati generalmente in una regione non codificata dei cromosomi cellulari. Il genoma umano è costituito da sequenze ripetute di DNA: le cd. STRs – *short tandem repeat* – sono individuate intorno alla struttura dei cromosomi nella zona strutturale centrale, componenti fondamentali per l'identificazione degli esseri umani. Cfr. Mastrangelo (2017), Galgani (2006), p. 40, Ricci (2001), pp. 108 e ss.

[39] Amato *et. al.* (2013), p. 39.

[40] Per un approfondimento si vedano tra gli altri Ricci (2018), p. 93; Rivello (2016), pp. 1521-1531; Ubertis (2016), pp. 1198 e ss.; Renzetti (2015), pp. 399 e ss.; Bargis (2011), pp. 49 e ss. Caprioli (2008), pp. 3523; Ferrua (2008), pp. 12 e ss.; Pulitanò (2006), p. 802.

a conoscenze tecnico-scientifiche[41]. L'utilizzo di leggi scientifiche per ricostruire i fatti da cui dipende la decisione sulla *res iudicanda* non trova nel diritto processuale una sua specifica regolamentazione. Il codice di rito penale prevede uno specifico mezzo di prova – la perizia – destinato ad essere ammesso «quando occorre svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze tecniche, scientifiche o artistiche» (art. 220, comma 1 c.p.p.). Laddove debbano essere adottate competenze del suddetto genere – e ricorrano le condizioni per l'ammissibilità d'ogni mezzo istruttorio, oltre a quella, peculiare, integrata dalla occorrenza dell'intervento da parte del "testimone esperto" – il disporre la perizia costituisce per il giudice un vero e proprio obbligo[42]. Tuttavia, secondo il vigente ordinamento processuale penale, l'espletamento della tipica attività istruttoria prevista dagli artt. 220 ss. c.p.p. non è l'esclusivo veicolo per l'ingresso in sede giudiziaria del sapere tecnico-scientifico: il modello conosce altresì l'istituto della consulenza tecnica di parte esperibile «fuori dai casi di perizia» (art. 233 c.p.p.). Ciascuna delle parti è pertanto legittimata a designare fino a due propri esperti, per essere da questi assistita, nelle questioni implicanti «specifiche competenze tecniche, scientifiche o artistiche», fin dalle indagini preliminari (artt. 359, 360, 391-bis ss. c.p.p.)[43].

Com'è noto, negli Stati Uniti alcune delle questioni più rilevanti connesse all'uso della prova scientifica sono state affrontate non solo a livello legislativo, ma anche giurisprudenziale[44]. I pilastri dell'orientamento giurisprudenziale statunitense in materia sono costituiti dai due *leading cases*. Innanzitutto il caso *Frye vs. United States*[45], deciso dalla Corte d'appello del distretto di Columbia e, in secondo luogo, la decisione *Daubert vs. Merrel Dow Pharmaceuticals*[46], disposta nel 1993 dalla Suprema Corte Federale. Inoltre, si segnalano le *Federal rules of evidence* del 1975 (in particolare le *rules* 702 e 703) aventi ad oggetto la *testimony by experts*. In particolare, la *Circuit Court del District of Columbia*, nel caso *Frye* del 1923, avente ad oggetto l'ammissibilità come prova dei risultati sperimentali dell'utilizzazione di un poligrafo (una primordiale "macchina della verità"), aveva indicato come parametro di valutazione dell'attendibilità della prova scientifica, quello del consenso della comunità scientifica di riferimento (cd. *general acceptance test*), così dichiarando inammissibile la richiesta istruttoria avanzata dalla difesa[47]. Tuttavia, tale criterio interpretativo non tardò a manifestare i suoi limiti, non solo perché in tal modo la prova scientifica "nuova", in quanto priva di un giudizio di *general acceptance*, avrebbe potuto essere ammessa – a prescindere dalla sua validità – ma anche e soprattutto per l'evidente ragione che il consenso della comunità scientifica non avrebbe potuto attribuire di per sé ad una tecnica di indagine l'idoneità a dimostrare i fatti oggetto di accertamento.

Successivamente, la *Federal Supreme Court* degli USA, nella sentenza del 28 giugno 1993 relativa al caso *Daubert*, fu investita del problema dell'ammissibilità di una prova scientifica fondata su principi che non apparivano sufficientemente consolidati da ricevere generale accoglienza nella comunità scientifica nello specifico campo di ricerca. La Corte ha indicato alcuni criteri per valutare l'ammissibilità delle prove scientifiche (e dunque a dare ingresso processuale anche alla cd. "scienza nuova") e, in sostanza a verificarne la validità e attendibilità. Il primo criterio elaborato dalla *Supreme Court* è quello della verificabilità ossia della falsificabilità della tecnica a fondamento della prova; il secondo criterio è rappresentato dalla sottoposizione della teoria o tecnica al controllo, alla revisione critica da parte degli altri membri della comunità scientifica (*peer review*) nonché dalla pubblicazione dei risultati delle relative ricerche su riviste specializzate (*publication*); il terzo (duplice) criterio richiede che il giudice, nel vagliare l'ammissibilità della prova scientifica, tenga conto della frequenza (o percentuale) di errore, conosciuta o potenziale, nonché della presenza di standard costanti di verifica, ossia dell'eventuale riscontro di una molteplicità di casi; ai menzionati criteri si deve poi naturalmente aggiungere quello del consenso generale da parte della comunità scientifica che, se non deve essere utilizzato quale strumento esclusivo di valutazione per l'ammissione della *expert*

[41] In particolare, O. Dominioni ha affermato che la prova scientifica «(…) è una espressione ellittica che designa un complesso fenomeno (…) si tratta di operazioni probatorie per le quali, nei momenti dell'ammissione, dell'assunzione e della valutazione, si usano strumenti di conoscenza attinti alla scienza ed alla tecnica». Dominioni, (2005), p. 12. Per un approfondimento sulla prova scientifica si veda anche Tonini (2010b), p. 321.
[42] Lorusso (2008), pp. 295 e ss.
[43] Forte (2018), p. 2267.
[44] Per un approfondimento si vedano tra gli altri Kaufman (2001): pp. 7-20; Graham (2000): pp. 322 e ss.; Barovick (1999), p. 1533; Graham (1992), p. 243.
[45] *Frye v. Unites States*, 293 F. 1013 (D.C. Cir., 1923).
[46] *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).
[47] Ossia quella di ammettere come prova nel processo la sottoposizione dell'imputato al test della macchina della verità.

scientific testimony, può comunque offrire conferme importanti in ordine alla validità di una teoria o tecnica scientifica che si intenda utilizzare nel processo. Il giudice, nell'analizzare tali prove, deve assumere il ruolo di "guardiano" ("*gatekeeper*"), cui è assegnato il compito di valutare l'affidabilità e la validità dei *methods and procedures* che presiedono alla formazione di ogni singola prova scientifica che le parti intendono dedurre nel processo.

I criteri individuati nel caso *Daubert* costituiscono, come riconosciuto dalla stessa Corte Suprema USA, massime o regole di esperienza, certamente idonee per le finalità perseguite, ma non definitivamente risolutive. Ad esse possono dunque ragionevolmente affiancarsi anche quelle che giurisprudenza e dottrina hanno ulteriormente proposto o vorranno proporre, naturalmente senza pretendere che i diversi criteri elaborati debbano ogni volta coesistere tra loro. Com'è noto, la nostra giurisprudenza di legittimità si è occupata di temi connessi alla valutazione di affidabilità della prova scientifica ma ha più volte dimostrato di riconoscere validità ai criteri elaborati dalla giurisprudenza statunitense[48].

Se il codice di procedura penale italiano odierno "contiene" in sé norme specifiche concernenti sia il momento dell'ammissione sia quello dell'acquisizione della perizia, non altrettanto si può affermare per quanto concerne la terza fase del procedimento probatorio: quello di valutazione dei corrispondenti risultati. L'articolo 192 c.p.p. dispone che «il giudice valuta la prova dando conto nella motivazione dei risultati acquisiti e dei criteri adottati». Domina, pertanto, l'idea per cui il giudice possa liberamente valutare gli esiti di quei procedimenti probatori che siano stati ammessi ed acquisiti legittimamente[49], purché siano adeguatamente motivati in sentenza quei risultati che ha ritenuto determinanti ai fini della decisione assunta, nonché delle massime d'esperienza impiegate nell'apprezzarli. Perciò, il giudice, obbligato a disporre la perizia – poiché imposta dall'esigenza di specifiche competenze scientifiche -, una volta che la perizia stessa sia stata eseguita, non è tenuto a decidere conformemente ai risultati della corrispondente procedura acquisitiva, fermo restando, però, l'obbligo di un'adeguata motivazione nella statuizione circa il suo diverso avviso[50]. A tal proposito, il giudice diviene *peritus peritorum*, il quale pur dovendo avvalersi di esperti, non è vincolato alle loro conclusioni e può disattenderle. Il magistrato, in ogni caso, deve essere in grado di "controllare" l'esperimento della prova scientifica, comprendere la "sintassi" del ragionamento e il percorso seguito dall'esperto per giungere alle sue conclusioni[51]; egli deve essere inoltre in grado di conoscere i limiti scientifici della prova, in modo da divenire fruitore consapevole della scienza che viene introdotta nel processo[52]: deve assumere cioè quel ruolo che la giurisprudenza americana ha definito di "*gatekeeper*"[53].

[48] Cass. Sez. 1, Sentenza n. 31456 del 21 maggio 2008 (dep. 29 luglio 2008) Rv. 240764, Franzoni, in tema di applicazione della *Bloodstain Pattern Analysis* - tipo di indagine che studia la morfologia e disposizione delle macchie ematiche rinvenute sugli oggetti presenti sul luogo del delitto, per verificare la provenienza dei colpi inferti alla vittima e la reciproca posizione di quest'ultima e dell'aggressore - la Corte ha evidenziato come nel caso specifico fossero stati rispettati «anche i rigorosi criteri di validazione della prova scientifica (aventi per l'A.G. italiana natura meramente orientativa) elaborati dalla giurisprudenza degli USA» (per un approfondimento cfr. Caprioli (2009), pp. 1867 e ss.); Cass., Sez. 4, Sentenza n. 43786 del 17 settembre 2010 (dep. 13 dicembre 2010) Rv. 248943 Cozzini, la quale ha intrapreso una vera e propria opera di ricostruzione dei criteri che il giudice di merito deve seguire nella valutazione della validità della prova scientifica, ispirandosi - pur senza farvi esplicito riferimento - alle linee guida dettate dalla giurisprudenza statunitense, ritenute questa volta non più solo meramente orientative ma del tutto vincolanti; Cass. Sez. 5, Sentenza n. 36080 del 27.03.2015 (dep. 7.09.2015), Knox, in motivazione (p. 35): «(…) un risultato di prova scientifica può essere ritenuto attendibile solo ove sia controllato dal giudice, quantomeno con riferimento all'attendibilità soggettiva di chi lo sostenga, alla scientificità del metodo adoperato, al margine di errore più o meno accettabile ed all'obiettiva valenza ed attendibilità del risultato conseguito». Ancora, secondo Cass. Sez. 2, Sentenza n. 12751 del 08/03/2011 Ud. (dep. 29/03/2011) Rv. 250049, Cutaia, le nuove metodologie su cui si fonda la "prova nuova" quale presupposto per la richiesta di revisione, devono essere «accreditate e ritenute pienamente attendibili dalla comunità scientifica». Inoltre, secondo Cass. N. 3031 del 22.10.2009, Allegro, l'accertamento peritale proposto con la richiesta di revisione, ove richieda il ricorso a «nuove tecniche e a nuove conoscenze», deve porsi come «il risultato di protocolli di indagine riconosciuti dalla comunità scientifica». Analogamente Cass. Sez. 6, Sentenza n. 34531 del 04/07/2013 Ud. (dep. 08/08/2013), Mazzagatti, in motivazione: «(…) deve ovviamente trattarsi di applicazioni tecniche accreditate e rese pienamente attendibili dal livello del sapere acquisito dalla comunità scientifica, dato che soltanto tale condizione conferisce un tasso di ragionevole affidabilità ai risultati della nuova indagine».

[49] Cfr. Cordero, (2012), p. 569; Cecchi (2017), pp. 915 e ss.; Tonini (2015), pp. 1410 e ss..

[50] In tal senso, Tonini, (2011), p. 364; inoltre, si veda Cass., Sez. IV, 13 dicembre 2010, n. 43785 in Guida Dir., 2011, n. 6 secondo la quale «quando il sapere scientifico non è consolidato o non è comunemente accettato perché vi sono tesi in irrisolto conflitto, spetta comunque al giudice prescegliere quella da preferire».

[51] Taruffo (2005), p. 1079: «(…) è necessario che il giudice sia in grado almeno di valutare la validità dei metodi di cui il consulente si è servito per svolgere il suo compito».

[52] Giova segnalare quanto affermato da O. Dominioni «non è consentito che nella funzione probatoria si usino apparati conoscitivi insuscettibili di controllo ad opera del giudice e delle parti», Dominioni (2005), p. 69.

[53] Come osservato da Cass. 36080/2015, Knox, cit., in motivazione (p.33): «La conseguenza dell'ineludibile presa d'atto di tale stato di legittima ignoranza del giudice, e dunque della sua incapacità di governare "autonomamente" la prova scientifica, non può, però, essere l'acritico affidamento, che equivarrebbe - anche per un malinteso senso del libero convincimento e di altrettanto malinteso concetto di "perito

2.1. *Prova scientifica e prova biometrica a confronto.*

Diverse sono le problematiche che emergono in seno al rapporto fra prova scientifica e prova biometrica. La prima affonda le sue radici da una previa questione terminologica che riguarderebbe l'uso alternativo dell'aggettivo "biometrico" sia per quel che concerne il dato biologico grezzo sia per il cd. *template*[54] (cfr. *supra*, § 1). La confusione nascerebbe da un uso sinonimico dell'aggettivo "biometrico" in riferimento al campione biologico rilevato per esempio sulla *scena criminis* e il dato contenuto all'interno del supporto digitale o ancora in relazione all'algoritmo utilizzato per il funzionamento del sistema di riconoscimento[55]. In ogni caso, sia ci si riferisca al campione biologico grezzo, sia si consideri il *template*, si ritiene che la prova biometrica costituisca una *species* del più ampio *genus* di "prova scientifica"[56]. A seconda, poi, della tipologia di tecnologia che viene utilizzata all'interno del processo penale (più o meno avanzata) si potrà operare un distinguo fra "prova scientifica" e "prova scientifica nuova"[57].

In secondo luogo, la biometria applicata al contesto forense ha fatto emergere dubbi riguardanti l'assoluta affidabilità dei risultati scaturenti dall'applicazione dei sistemi di identificazione[58]. Parte della dottrina ha sostenuto l'alto grado di attendibilità, ritenuto prossimo alla certezza e la compatibilità con gli standard "Daubertiani" probatori richiesti in tale sede (cfr. *supra*, § 2.1), dei metodi scientifici ad esse sottesi e della controllabilità oggettiva delle modalità di formazione del dato cognitivo. Dall'altra parte, un margine di errore nei sistemi di identificazione o autenticazione, come per qualsiasi sistema statistico di comparazione, risulta pur sempre presente e come tale è suscettibile di creare problematiche in ambito processuale[59]. I cambiamenti delle condizioni ambientali e di registrazione e acquisizione dei dati, così come i cambiamenti fisici (temporanei o permanenti) o il tempo intercorrente tra l'*enrollment* e la comparazione biometrica, giocano un ruolo fondamentale, riducendo le possibilità di riconoscimento. Peraltro, la disciplina biometrica si basa tipicamente su leggi di tipo statistico che consentono di elaborare previsioni sull'incertezza del risultato, ma non di accertare i fatti: è noto il dibattito relativo ai rapporti tra scienze statistiche e accertamento penale[60].

Oltre a ciò, si ritiene che in tutti i casi in cui le tecniche di identificazione biometriche richiedano il prelievo di materiale biologico grezzo dalla persona sottoposta alle indagini o, a fortiori, di terzi al procedimento, si pongano problematiche relative alla compatibilità coi principi costituzionali eretti a tutela dei diritti fondamentali dell'uomo[61] (il diritto alla dignità, alla libertà personale, alla salute e, secondo parte della dottrina, il diritto di difesa)[62]. Si aggiunga altresì il rischio intrinseco legato all'adozione di tali metodi di indagine in relazione all'oggetto su cui vertono, di cagionare una lesione al diritto alla riservatezza dei dati personali[63], considerato nella duplice componente positiva ad esercitare una verifica sulla correttezza e sulla circolazione dei dati e in quella negativa riguardante il diritto di escludere dalla fruizione del dato tutti i soggetti che ne sono titolari[64].

Si può, inoltre, sostenere che sia ravvisabile un problema di compatibilità del procedimento tecnico-scientifico volto all'analisi e alla comparazione dei dati con le fasi in cui si articola solitamente il processo penale, e, in particolare, un problema di inquadramento delle singole

dei periti" - a sostanziale rinuncia al proprio ruolo, mediante fideistica accettazione del contributo peritale, cui delegare la soluzione del giudizio e, dunque, la responsabilità della decisione». Per un approfondimento sul ruolo del giudice tra gli altri cfr. Bartoli (2018), p. 12.

[54] Cfr. *supra*, § 1.2.

[55] Cfr. Presidenza del Consiglio dei Ministri - Comitato Nazionale per la Bioetica (2010), p. 6, *http://bioetica.governo.it/media/1846/p95_2010_identificazione-corpo-umano-biometria_it.pdf* (ultima visualizzazione il 28/2/2019).

[56] Il *template* inteso come dato biologico contenuto in un supporto digitale è considerato non solo "prova biometrica" ma anche "digitale" definita dallo *Scientific Working Group on Digital Evidence* come qualsiasi informazione con valore probatorio, che sia o meno memorizzata o trasmessa in un formato digitale (cfr. https://www.swgde.org/- ultima visualizzazione il 19/2/2019). Per un approfondimento si veda Daniele (2011), pp. 297 ss.

[57] Dominioni (2005), pp. 83 e ss.

[58] Fanuele (2009), pp. 1-2.

[59] Ad esempio, gli errori compiuti da un sistema per il riconoscimento del volto sono generalmente maggiori di quelli riscontrabili in sistemi basati sul riconoscimento delle impronte digitali o dell'iride.

[60] Per un approfondimento si veda tra gli altri Blaiotta (2010).

[61] Emerge l'esigenza di un bilanciamento delle esigenze connesse all'accertamento dei reati con la tutela dei diritti di rango costituzionale, come il diritto alla dignità personale, alla libertà, alla salute e alla riservatezza. Cfr. Fanuele (2009), p. 38; Felicioni (2007), p. 16; Kostoris (2006), p. 330.

[62] Per una riflessione volta ad individuare le possibili ricadute tra indagine genetiche e garanzia del diritto di difesa, Felicioni (2007), p. 26 e Giunta (2014), p. 568.

[63] Sellaroli (2006), p. 71.

[64] Cfr. tra gli altri Quattrocolo (2019), pp. 2 e ss.; Allegrezza (2007), p. 65; Bonetti (2003), p. 11.

attività scientifiche preposto alla formazione del dato cognitivo all'interno della cornice dei mezzi di prova catalogati all'interno del codice del 1988. Un esempio paradigmatico delle difficoltà che si pongono al giurista interprete nell'opera di armonizzazione delle tecniche di identificazione biometrica con i paradigmi del processo penale è rappresentato dalla disciplina della dattiloscopia[65]. Tale metodo di riconoscimento si snoda in due fasi principali: la prima volta al rilevamento dell'impronta digitale mediante l'impiego di tecniche che si differenziano in ragione della morfologia della traccia rinvenuta, mentre la seconda fase è preordinata alla comparazione dell'impronta rinvenuta in sede di rilievi sulla *scena criminis* con quella prelevata dalla persona sottoposta alle indagini[66]. Inquadrando l'attività tecnico-scientifica nella cornice processuale, ferma la previsione dell'articolo 349 comma 2 c.p.p., che menziona gli accertamenti dattiloscopici della polizia giudiziaria in sede identificativa, si segnala un contrasto interpretativo. Da un lato, la giurisprudenza tende a ricondurre entrambe le fasi di rilevazione e comparazione delle impronte all'interno dell'articolo 354 commi 2 e 3 c.p.p., in forza del loro carattere meramente materiale. Dall'altra, parte della dottrina propone una distinzione tra le due fasi, qualificando il *matching* come un'attività di carattere valutativo da espletarsi nelle forme della consulenza (*ex* art. 360 c.p.p.) o nelle forme della perizia. La risoluzione della questione non può di certo prescindere dalla correttezza della summenzionata distinzione fra operazione di carattere materiale (riferibili alla nozione di "rilievo") e le attività di carattere valutativo inquadrabili nell'espressione codicistica di "accertamento tecnico". Va inoltre osservato che il distinguo prospettato non permette l'applicazione in ogni caso del corredo di garanzie difensive fornite dall'articolo 360 c.p.p. la cui operatività va circoscritta agli accertamenti tecnici (e non ai rilievi materiali) non procrastinabili al dibattimento per cause relative alla deteriorabilità dell'oggetto di indagine in seguito alle attività di analisi[67]. Dunque, nel caso in cui si vogliano acquisire tali elementi di prova nel processo affinché il giudice possa valutarli, occorrerà procedere con le forme della consulenza e della perizia che garantiscono la salvaguardia del principio del contraddittorio nonché la controllabilità del metodo prescelto con riguardo alla morfologia dell'impronta rinvenuta e del rispetto dei criteri valutativi relativi all'attività di *matching*[68].

3. Conclusioni

Con il presente contributo si è cercato di presentare e descrivere i principali caratteri della disciplina tecnico-scientifica denominata "biometria" che ha come scopo quello di automatizzare le procedure di identificazione o di verifica dell'identità, attraverso la valutazione di caratteristiche fisiche e/o comportamentali degli esseri umani, acquisite da sensori elettronici, elaborate da specifici algoritmi matematici e, infine, trasformate in modelli matematici. La scienza biometrica, come altre, non è priva di errori, a maggior ragione se si considera la sua natura tipicamente statistico-probabilistica. L'introduzione sistematica di tecnologie biometriche all'interno del processo penale, potrebbe, pertanto, comportare alcune problematiche in termini di affidabilità dei risultati scaturenti dalla loro applicazione e di compatibilità fra la disciplina in esame, i principi costituzionali e le tipiche garanzie processuali. Tuttavia, a seguito del notevole sviluppo tecnologico recente, il processo penale pare non poter più fare a meno dei contributi offerti dalla biometria, soprattutto perché sia la scienza sia il processo, anche se con diversi approcci, hanno il comune obiettivo della ricostruzione del nesso causale. I dati biometrici devono essere analizzati e valutati in termini di "accuratezza scientifica" e si deve caso per caso comprendere quale tipo di "valore" accordare loro.

I rischi più determinanti in capo alla scienza forense nella sua recente dimensione digitale e nei suoi approfondimenti di studio sulla biometria, stanno a poco a poco trasformando il

[65] Non è, infatti, possibile dar conto, in questa sede, di tutti i limiti relativi ai metodi di identificazione riportati nei paragrafi precedenti né della parabola evolutiva percorsa dalla tecnologia in riferimento ai singoli sistemi di riconoscimento.
[66] La giurisprudenza richiede che vi siano almeno diciassette punti di coincidenza affinché il risultato identificativo sia utilizzabile in sede penale.
[67] Sulla nozione di irripetibilità si vedano Cesari (1999), p. 8 e Ichino (1992), p. 45.
[68] Si ritiene che la medesima interpretazione pare ispirare altresì la disciplina di un'altra prova biometrica, quella del DNA, inquadrabile nella cornice della consulenza tecnica e della perizia. L'inquadramento di tale mezzo di prova è reso complesso, da un lato, dalla varietà delle tecniche di analisi dei vari profili genetici e, dall'altro, dall'attitudine della disciplina a comprimere diritti di rilevanza costituzionale. Per un approfondimento sulla prova genetica si veda Fanuele (2009), pp. 95 e ss., Felicioni (2009), pp. 6-24.

sistema attuale della giustizia penale. In questo senso, è auspicabile un intervento legislativo chiarificatore teso a uniformare la disciplina e che distingua un dato biometrico da un altro, e le differenti applicazioni che possono essere messe in atto, dal momento che la specificità di ciascun dato e degli ambiti di impiego impone soluzioni giuridiche differenziate. Altrimenti, il pericolo è quello dell'affievolirsi notevolmente delle garanzie processuali (come per esempio il principio del contraddittorio, quello della ragionevole durata del processo nonché del diritto alla difesa) oltre ad alcune problematiche legate a più ampie garanzie individuali come il diritto alla riservatezza. Peraltro, uno degli obiettivi principali del Garante privacy è quello di limitare l'utilizzo di tali tipologie di dati attraverso il ricorso a mezzi alternativi di autenticazione e identificazione meno invasivi della sfera personale e della libertà individuale, sussistendo un'inderogabile esigenza di rispettare il corpo umano, salvo sia strettamente necessario e conforme al principio di proporzionalità, procedere diversamente[69].

A conclusione di queste brevi riflessioni suonano quanto mai profetiche le parole di Stefano Rodotà al proposito: «L'unità della persona può essere ricostruita solo estendendo al corpo elettronico il sistema di garanzie costruito per il corpo fisico»[70].

Bibliografia

Allegrezza, Silvia (2007): "Giustizia penale e diritto all'autodeterminazione dei dati personali nella regione Europa", in Negri Daniel (eds.): *Protezione dei dati personali e accertamento penale* (Roma, Aracne editore), pp. 59-85

Amato Salvatore, Cristofari Fabiana, Raciti Salvatore (2013): *Biometria. I codici a barre del corpo* (Torino, Giappichelli)

Balossino Nello e Siracusa Simona (2004): *L'identificazione basata sul volto: metodi fisionomici e metrici* (Milano, Itasforum)

Bargis, Marta (2011): "Note in tema di prova scientifica nel processo penale", *Rivista di diritto processuale*, 66 (1), pp. 49 – 66

Barovick Robin (1999): "Between Rock and Hard Place: Poligraph Prejudice Persist After Scheffer", *Buffalo Law Review*, 47, pp. 1533 e ss.

Bartoli, Roberto (2018): "Diritto penale e prova scientifica" in Canzio Giovanni e Luparia Luca (eds.), *Prova scientifica e processo penale* (Milano, Wolters Kluwer-Cedam), pp. 75-115

Bisi, Silvia (2005): "Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica", *Ciberspazio e diritto*, 6 (4), pp. 3-35

Blaiotta, Rocco (2010): *Causalità giuridica* (Torino, Giappichelli)

Bonetti, Michele (2003): *Riservatezza e processo penale* (Milano, Giuffrè)

Caprioli, Francesco (2009): "Scientific evidence e logiche del probabile nel processo per il 'delitto di Cogne'", *Cassazione penale*, 5, pp. 1867 e ss.

Caprioli, Francesco (2008): "La scienza 'cattiva maestra': le insidie della prova scientifica nel processo penale", *Cassazione penale*, 9, p. 3523.

Cecchi, Marco (2017): "L"autonoma valutazione del giudice' quale baluardo contro l'appiattimento sulla prova scientifica", *Diritto Penale e Processo*, 7, pp. 915-924

Cesari, Claudia (1999): *L'irripetibilità sopravvenuta degli atti di indagine* (Milano, Giuffrè)

Cordero, Franco, (2012): *Procedura penale* (Milano, Giuffrè)

[69] Cfr. art. 9 del Regolamento (UE) n. 2016/679.
[70] Rodotà (2006), pp. 3-24.

Cuomo, Luigi (2014): "Profili giuridici del trattamento biometrico dei dati", *Rivista Italiana di Medicina Legale e del Diritto in campo sanitario*, 1, p. 43

Daniele, Marcello (2011): "La prova digitale nel processo penale", in *Rivista di diritto processuale*, pp. 297 ss.

Dominioni, Oreste (2015): "L'esperienza italiana di impiego della prova scientifica nel processo penale", *Diritto Penale e Processo*, 5, p. 601

Dominioni, Oreste (2005): *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione* (Milano, Giuffrè)

Fanuele, Chiara (2009): *Dati genetici e procedimento penale* (Padova, Cedam)

Felicioni, Paola (2016): Il regolamento di attuazione della banca dati nazionale del DNA: scienza e diritto si incontrano, *Diritto penale e processo*, 6, pp. 724 - 742

Felicioni, Paola (2009): "L'Italia aderisce al Trattato di Prum: disciplinata l'acquisizione e l'utilizzazione probatoria dei profili genetici", *Diritto penale e processo*, 2 (2), pp. 6-24

Felicioni, Paola (2007): *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico* (Milano, Ipsoa)

Ferrua, Paolo (2008): "Metodo scientifico e processo penale", *Diritto penale e processo*, 6, pp. 12-19

Forte, Luca (2018): "Il ruolo della perizia nel processo penale tra neutralità della prova e prova decisiva: una difficile collocazione", *Giurisprudenza Italiana*, 10, p. 2267

Galgani, Benedetta (2003): "Un test di elevata scientificità e un inedito banco di prova per la 'civiltà' del processo" in Chiavario, Mario (eds.) *Nuove tecnologie e processo penale* (Torino, Giappicchelli), pp. 40-50

Giunta, Fausto (2014): *Questioni scientifiche e prova scientifica tra categorie sostanziali e regole di giudizio*, (Pisa, Edizioni ETS)

Graham, Michael (2000): "The Expert Witness Predicament: Determing 'Reliable' Under the Gatekeeping Test of Daubert, Kuhmo, and Proposed Amended Rule 702 of Federal Rules of Evidence", *University of Miami Law Review*, 317, pp. 322 e ss.

Graham Michael (1992): *Federal Rules of Evidence. A Nutshell* (St. Paul Minn., Thomson West)

Grimaldi Mirko, D'Apolito Sonia, Fivela Gili Barbara, Sigona Francesco (2014): "Illusione e scienza nella fonetica forense: una sintesi", *Mondo Digitale*, 13 (53), pp. 1-9

Ichino, Giovanna (1992): "Gli atti irripetibili e la loro utilizzazione dibattimentale", in Ubertis, Giulio (eds.): *La conoscenza del fatto nel processo penale* (Milano, Giuffrè), pp. 110 e ss.

Iovane, Gerardo (2008): *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza* (Roma, Aracne)

Kaufman, Robert (2001): "The expert witness. Neither Frye nor Daubert solved the problem: what can be done?", *Science & Justice*, 41, 1, pp. 7-20

Kostoris, Roberto E. (2006): "Prelievi biologici coattivi" in KOSTORIS Roberto E. e ORLANDI Renato (eds.): *Contrasto al terrorismo interno e internazionale* (Torino, Giappichelli), pp. 329 e ss.

La Regina, Katia (2018): "Riconoscimento della voce – brevi note sul riconoscimento della voce nel processo penale", *Giurisprudenza Italiana*,1, 212

Lorusso, Sergio (2008): "La prova scientifica" in Gaito, Alfredo (eds.): *La prova penale*, (Milano, Utet), pp. 295 e ss.

Masera, Luca (2007): "Il giudice penale di fronte a questioni tecnicamente complesse: spunti di riflessione sul principio dello iudex peritus peritorum - Il commento", *Il Corriere del Merito*, 3 (3), pp. 351-355

Mastrangelo, Nicolina (2017): "Profiling del DNA: una rivoluzione chiamata PCR e STRs", *Criminalistica*, (http://crimint.it/profiling-del-dna-una-rivoluzione-chiamata-pcr-e-strs/)

Mastronardi, Giuseppe (2014): "Identificazione personale mediante il confronto di volti", *Mondo Digitale,* pp. 1-12

Moscarini, Paolo (2016): "Lo statuto della 'prova scientifica' nel processo penale", *Diritto Penale e Processo*, 6, pp. 649 e ss.

Preite, Gianpasquale (2016): *Politica e biometria. Nuove prospettive filosofiche delle scienze sociali* (Trento, Tangran edizioni scientifiche)

Preite, Gianpasquale (2007): *Il riconoscimento biometrico. Sicurezza versus Privacy* (Trento, Ed. UNI Service)

Pulitanò, Domenico (2006): "Il diritto penale fra vincoli di realtà e sapere scientifico", in *Rivista italiana di diritto processuale penale*, 49 (3), pp. 795-825

Quattrocolo, Serena (2019): "Equità del processo penale e automated evidence alla luce della convenzione europea dei diritti dell'uomo", *Rivista Italo-Spagnola di Diritto Processuale*, 1, pp. 1-17

Renzetti, Silvia (2015): "La prova scientifica nel processo penale: problemi e prospettive", *Rivista di Diritto Processuale*, 2, pp. 399 e ss.

Ricci Cristoforo e Ricci Pietrantonio (2018): "Le biobanche di ricerca: questioni e disciplina", *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)*, 1, p. 93

Ricci, Ugo (2001): *Dna e crimine: dalla traccia biologica all'identificazione genetica* (Roma, Laurus Robuffo)

Rivello, Pierpaolo (2016): "Alcune osservazioni in ordine alla banca dati nazionale del DNA", *Diritto penale e processo*, 11, pp. 1521-1531

Rodotà, Stefano (2006): "Trasformazioni del corpo", *Politica del diritto*, 1, pp. 3-24

Seckiner Dilan, Mallett Xanthé, Maynard Philip, Meuwly Didier, Roux Claude (2019): "Forensic gait analysis – Morphometric assessment from surveillance footage", *Forensic Science International*, 296, pp. 57-66

Sellaroli, Valentina (2006): "Analisi del Dna e processo: in quale senso è una novità?" in CHIAVARIO, Mario (eds.): *Nuove tecnologie e processo penale* (Torino, Giappicheli), pp. 70 e ss.

Taruffo, Michele (2005): "La prova scientifica nel processo civile", *Rivista trimestrale di diritto processuale civile*, 4, p. 1079

Terraciano, Ugo (2014): *La metodologia dell'investigazione* (Milano, Franco Angeli)

Tistarelli Massimo e Champod Christophe (2017): *Handbook of Biometrics for Forensic Science* (Cham, Springer)

Tonini, Paolo (2015): "Nullum iudicium sine scientia. Cadono vecchi idoli nel caso Meredith Kercher", *Diritto Penale e Processo*,11, pp. 1410 e ss.

Tonini, Paolo (2011): "Dalla perizia 'prova neutra' al contraddittorio sulla scienza", *Diritto Penale e Processo*, 3, p. 361

Tonini, Paolo (2010a): "La Cassazione accoglie i criteri Daubert sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza", *Diritto penale e processo*, 11, pp. 1341 e ss.

Tonini, Paolo (2010b): *Manuale di procedura penale* (Milano, Giuffrè)

Ubertis, Giulio (2016): "Prova scientifica e giustizia penale", *Rivista italiana di diritto processuale penale*, pp. 1198 ss.

Valli, Roberto (2013): *Le indagini scientifiche nel procedimento penale* (Milano, Giuffrè)

Vanacore, Giorgio (2015): "Sapere scientifico e processo giudiziario", *Danno e Responsabilità*, 6, pp. 645 e ss.

Wayman James, Jain Anil, Maio Dario (2005): *Biometric Systems. Technology, Design and Performance Evaluation* (New York, Springer)

Wilkins, Jonathan (2019): "Can biometrics secure manufacturing?", *Biometric Technology Today*, 1, pp. 9-11

Yoruk Erdem, Kokukoglu Ender, Sankur Bulent (2006): "Shape-Based Hand Recognition", *IEEE Transaction on Image Processing*, 15 (7), pp. 1083-1815

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

http://dpc-rivista-trimestrale.criminaljusticenetwork.eu