UNIVERSITÀ DEGLI STUDI DI TORINO

DIPARTIMENTO DI GIURISPRUDENZA

CORSO DI DOTTORATO IN "DIRITTI E ISTITUZIONI"

CICLO: XXXIV

AUTOMATED BIOMETRIC RECOGNITION SYSTEMS E PROCEDIMENTO PENALE.

INDAGINE SUI FONDAMENTI E SUI LIMITI DELL'IMPIEGO DELLA BIOMETRIA MODERNA A FINI GIUDIZIARI

CANDIDATA

Ernestina Sacchetto

SUPERVISORI

Chiar.ma Prof.ssa Serena Quattrocolo

Chiar.ma Prof.ssa Barbara Lavarini

Chiar.mo Prof. Francesco Caprioli

COORDINATRICE DEL DOTTORATO

Chiar.ma Prof.ssa Ilenia Massa Pinto

Anni Accademici: 2018/2019, 2019/2020, 2020/2021

SETTORE SCIENTIFICO-DISCIPLINARE: IUS/16 DIRITTO PROCESSUALE PENALE

INDICE

CAPITOLO III

"*POLICY BEFORE TECHNOLOGY*": L'IMPIEGO DEGLI *AUTOMATED BIOMETRIC RECOGNITION SYSTEMS* NELLO SPETTRO DELLE GARANZIE FONDAMENTALI DELLA PERSONA

CAPITOLO IV

AUTOMATED FACIAL RECOGNITION TECHNOLOGY E PROCEDIMENTO PENALE ITALIANO: SCENARI PRESENTI E FUTURI

INTRODUZIONE

Il lavoro si occupa di studiare gli *automated biometric recognition systems* in grado di comparare suoni, voci, immagini, impronte o altre informazioni, divenuti ormai di estremo rilievo per l'accertamento penale. A seguito del notevole, recente sviluppo tecnologico, infatti, il procedimento penale pare non poter più fare a meno dei contributi offerti dalla biometria. Per tale ragione, in via preliminare, verrà eseguita una rapida rassegna delle caratteristiche salienti del funzionamento dei sistemi di riconoscimento. Il primo approccio sarà dunque meramente descrittivo. Verranno tracciate alcune fondamentali distinzioni delle varie tecniche sulla base di ciò che concretamente consentono di compiere agli organi inquirenti, posto che esse sono talora in grado di attribuire alle forze dell'ordine facoltà estranee alla dimensione umana. Nella prima parte, quindi, si offre una panoramica delle principali caratteristiche della biometria moderna, con l'obiettivo di cogliere, nel loro insieme, le più attuali evoluzioni tecnologiche della materia in questione, anticipando alcune problematiche emergenti dalla sua applicazione nel procedimento penale. In particolare, a partire da necessarie precisazioni semantiche rispetto alle definizioni e ai principi sanciti nei documenti normativi di riferimento ed evidenziando sin da subito alcune idiosincrasie, si passerà all'esposizione delle diverse fasi di quello che può essere definito come cd. "ciclo della prova biometrica", corredato dalle relative misure di accuratezza che i vari sistemi di riconoscimento possono presentare in livelli differenti e le tre modalità applicative di *verifica*, *identificazione* e *categorizzazione*.

Si è inteso dedicare poi parte del capitolo successivo alla rappresentazione digitale del tratto biometrico ovvero al suo cd. modello elettronico o *template*. A tal proposito saranno operati significativi inquadramenti entro alcune categorie dogmatiche processuali tradizionali, fornendo al lettore i parametri utili per la comprensione della sua analisi nello spettro delle garanzie processuali fondamentali. L'analisi dei tratti biometrici digitalizzati coinvolge le più differenti discipline: dalla biologia alla statistica, dalla fisica all'informatica. Ma si tratta solo del livello più basilare di complessità: su questo si innesta infatti l'eventuale natura digitale del dato. Ulteriore livello di difficoltà è rappresentato poi dalla diffusione applicativa al fenomeno processuale penale di processi automatizzati. Il procedimento di *identificazione*, *autenticazione* o *categorizzazione* di un individuo, risulta oltremodo agevolato dall'impiego di tecniche di apprendimento automatico, le quali consentono di estrarre e analizzare caratteristiche fisiche, fisionomiche o comportamentali non direttamente visibili, favorendo in questo modo confronti e valutazioni metriche. Tuttavia i sistemi automatizzati di riconoscimento, sui quali oggi sono applicate tali tecniche, potrebbero

restituire risultati errati a causa di problematiche di "apprendimento" da parte dell'algoritmo ovvero per la presenza di un difetto di *training* dei propri modelli decisori. L'introduzione sistematica di alcuni software di riconoscimento biometrico all'interno del procedimento penale potrebbe generare diversi dubbi in termini di affidabilità dei risultati scaturenti dalla loro applicazione e di compatibilità fra la disciplina in esame, i principi costituzionali e i diritti processuali fondamentali. Garanzie quali la libertà personale, l'equo processo e il diritto alla riservatezza sono solo alcuni dei parametri che saranno impiegati per valutarne la legittimità. A tal proposito, il capitolo III affronterà dapprima l'analisi del dato biometrico entro i crismi classici della categoria processuale della "prova scientifica", considerando in particolare la capacità semantico-dimostrativa di un *match* scaturente da un software automatico di riconoscimento rispetto ai fatti oggetto di prova, per poi passare alla trattazione dell'impiego dello stesso nello spettro delle garanzie fondamentali poste a tutela dell'indagato/imputato.

Le definizioni di base e la ricostruzione tecnica fornite nei primi capitoli saranno utili per comprendere e analizzare le peculiarità delle più specifiche tecniche di riconoscimento facciale, sia rispetto al tratto del volto in sé considerato, sia con riferimento al *match* scaturente da una comparazione automatica eseguita tramite software. Come noto, una tecnologia particolarmente insidiosa e invasiva nella vita privata delle persone è rappresentata dalle telecamere di videosorveglianza impiegabili - sia all'interno del domicilio privato sia negli spazi pubblici - per acquisire informazioni utili alle indagini ovvero costituire un'importante prova in dibattimento. A maggior ragione, questo vale per le telecamere in grado di compiere l'ulteriore funzione di riconoscere gli individui presenti in una data area geografica. La disamina dell'*automated facial recognition system* offrirà così lo spunto per alcune riflessioni conclusive in merito alla prospettiva attuale e futura di impiego di queste peculiari e inedite tecnologie, alla luce dei più recenti documenti normativi sovranazionali.

Sul piano metodologico, il lavoro farà ricorso a diversi schemi e tabelle illustrative, di ausilio per il ragionamento logico e giuridico, al fine di facilitare la lettura e la comprensione di alcuni dei passaggi più tecnici dell'elaborato.

CAPITOLO I

DAL CAMPIONE BIOLOGICO GREZZO ALLA RAPPRESENTAZIONE DIGITALE E AL *TEMPLATE*: UN QUADRO TEORICO PER UNA DISCUSSIONE MULTIDISCIPLINARE SU BIOMETRIA E PROCESSO PENALE*

«*Identity is inseparable from the human personality. An identity is a statement of who an individual is. Our identities define who we are. They express what we would wish the world to know us as*»[1].

D. Chandrachud

SOMMARIO: - 0. Metodologia. - 1. *βίος* e *μέτρον*: una ricostruzione semantica della disciplina. - 1.1. Il trattamento dei dati biometrici e la direttiva 2016/680/UE. - 1.2. Proprietà dei tratti biometrici. - 2. Il "ciclo della prova biometrica": dal corpo "fisico" al corpo "elettronico". - 2.1. Modello analitico di riferimento. - 2.2. Dall'*enrollment* al *template*: il procedimento di digitalizzazione e binarizzazione biometrica. - 2.3. (*Segue*) La fase del *matching*. - 2.4. Le modalità di *verifica*, *identificazione* e *categorizzazione* biometrica. - 2.5. Tipologie di errore. - 3. Le tecnologie biometriche. Cenni sul differente potenziale carattere distintivo o tipico dei tratti biometrici. - 3.1. Le impronte digitali. - 3.2. Il riconoscimento della geometria della mano e l'impronta palmare. - 3.3. Il riconoscimento del volto. - 3.3.1. Cenni sul sistema A.F.I.S.-S.S.A. - 3.4. La misurazione dell'iride e della retina. - 3.5. Il riconoscimento basato su aspetti dinamici. - 3.5.1. Il riconoscimento vocale: una ricostruzione dello stato dell'arte. - 3.5.2. L'andatura del passo. - 3.5.3. Il riconoscimento dinamico della firma. - 3.6. Cenni in materia di genetica forense. - 3.6.1. Dal campione biologico grezzo alla sua conversione in *template*: la fase di "repertazione". - 3.6.2. Il prelievo a scopi identificativi: la l. 85/2009 a più di dieci anni dalla sua entrata in vigore. - 3.6.3. La banca nazionale del Dna e il laboratorio centrale. - 4. Spunti di riflessione sulle banche dati tecnico-scientifiche a uso forense.

---

* Il presente capitolo è costituito in parte da contributi sottoposti a *peer review* e già pubblicati, v. E. Sacchetto, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2/2019, E. Sacchetto, *Biometrics as forensic evidence: some reflections from the Italian Criminal proceeding's point of view*, *8th International Workshop on Biometrics and Forensics (IWBF)*, 2020, E. Sacchetto, *Face to face*: *il complesso rapporto tra automated facial recognition technology* e processo penale in *www.lalegislazionepenale.it*, 16.10.2020, E. Sacchetto, *Brevi riflessioni sui fondamenti e sui limiti del rapporto fra automated faced-based human recognition technology e processo penale*, *ASTRID*, 2022 (in via di pubblicazione) e E. Sacchetto, *Automated faced-based human recognition technologies e procedimento penale alla luce della proposta di regolamento sull'IA: alcuni spunti di riflessione*, in AA.VV., *Collana del Centro Studi Giuridici* del Dipartimento di Economia di Ca' Foscari, (a cura di) C. Camardi, atti del Convegno **"***La via europea per l'intelligenza artificiale*", Venezia il 25-26.11.2022 (in via di pubblicazione). Si ringraziano il Prof. Didier Meuwly (*University of Twente-Netherlands Forensic Institute*), il Prof. Avi Domb (*The Hebrew University of Jerusalem*), il Prof. Joseph Almog (*The Hebrew University of Jerusalem*), il Prof. Azi Zadock (*The Hebrew University of Jerusalem*), la Dott.ssa Sharon Brown (*Israel Police*), l'Ing. Giacomo Rogliero (*Direttore Tecnico Principale presso il Ministero dell'Interno*), il Dott. John Riemen (*Lead Specialist Center for Biometrics, Dutch Police*), la Prof.ssa Serena Quattrocolo (*Università del Piemonte Orientale "A. Avogadro"*), la Prof.ssa Barbara Lavarini (*Università degli studi di Torino*) e il Prof. Francesco Caprioli (*Università degli studi di Torino*) per le riflessioni confluite nel presente lavoro.

[1] Dissenting Opinion, Giudice *Justice Puttaswamy v. Union of India*, sentenza del 26 settembre 2018 (D.N. 35071/2012), Corte Suprema indiana, par. 179.

Metodologia

Alcune considerazioni preliminari e di carattere generale offriranno una pur sintetica *actio finium regundorum*, essendo l'intenzione quella di presentare un'istantanea dell'attuale rapporto fra le tecnologie biometriche di riconoscimento e il procedimento penale. Una ricostruzione tecnica è fondamentale nel delineare il quadro della ricerca. Uno degli obiettivi del presente studio sarà infatti quello di analizzare i tratti comuni della materia ed evidenziarne i limiti ancora sussistenti, concentrando l'attenzione su un dibattuto caso di studio, l'*automated facial recognition system* (cfr. *infra* il capitolo IV).

Con questo primo capitolo introduttivo si cercherà di presentare e descrivere i principali caratteri della disciplina tecnico-scientifica denominata "biometria", che ha come scopo - *inter alia* - quello di automatizzare le procedure di identificazione, verifica dell'identità e categorizzazione, attraverso la valutazione di caratteristiche fisiche, fisiologiche e/o comportamentali degli esseri umani, acquisite da sensori elettronici, elaborate da specifici algoritmi matematici e, infine, trasformate in immagini digitalizzate e/o in modelli elettronici (cd. "*template*")[2]. La scienza biometrica, come si approfondirà meglio *infra*, non è priva di errori, a maggior ragione se si considera la sua natura tipicamente statistico-probabilistica. L'impiego ormai sistematico di processi automatizzati da parte delle forze di polizia, all'interno del procedimento penale, può comportare alcune problematiche in termini di affidabilità dei risultati scaturenti dalla loro applicazione e di compatibilità fra la disciplina biometrica 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, tra gli altri, il comune obiettivo della ricostruzione di un nesso causale. I dati biometrici devono essere analizzati e valutati in termini di "accuratezza scientifica" e si deve comprendere caso per caso quale tipo di "valore" accordare loro. In questo senso, un primo approdo della ricerca è senz'altro costituito dall'auspicio di un intervento legislativo chiarificatore, teso a uniformare la disciplina, distinguendo un dato biometrico da un altro, nonché le differenti applicazioni che possono essere poste in atto, dal momento che la specificità di ciascun dato e gli ambiti di impiego impongono ormai soluzioni giuridiche differenziate. Ad oggi, i sistemi di riconoscimento più utilizzati nell'ambito del processo penale sono quelli basati su tratti quali le impronte digitali, le tracce foniche, la firma grafometrica, i

[2] Da questo momento in poi i termini "*template*" e "modello elettronico" verranno impiegati alternativamente come sinonimi. L'espressione "dato biometrico digitalizzato", che si avrà modo di illustrare meglio *infra* al § 2.2, invece, ricomprende le categorie di "immagine digitalizzata", "rappresentazione digitalizzata", e "rappresentazione digitale di un dato biometrico" ovvero di "t*emplate*" o "modello elettronico".

calcoli antropometrici e, naturalmente, la traccia genetica. Quest'ultima fondamentale informazione, come si vedrà, è l'unica ad essere stata regolamentata e iscritta entro i tradizionali istituti e garanzie fondamentali del processo penale, in tutto il suo "ciclo di vita" biometrico, dall'acquisizione del campione biologico grezzo o del reperto, all'analisi del profilo del Dna e, infine, alla trasposizione in modello elettronico a fini di comparazione. In tal senso si ritiene del tutto ragionevole che la legge n. 85 del 2009 possa essere considerata un primo valido punto di partenza per la compiuta disciplina di altri sistemi di riconoscimento biometrico, in cui si tenga ragionevolmente conto delle analogie ma soprattutto delle differenze fra i singoli dati. Al momento, come si approfondirà meglio *infra* al capitolo IV, i sistemi biometrici più controversi sono quelli di *automated facial recognition,* il cui impiego sta scatenando ampi dibattiti multidisciplinari a livello sia nazionale che sovranazionale. Infatti, risultano sempre più diffusi sistemi automatici o semi-automatici di intelligenza artificiale che permettono di riconoscere, con un certo grado di probabilità, l'identità di un determinato soggetto ignoto sulla base di una immagine del suo volto, sia in fotografia, sia registrata in un *frame* ricavato da una videoripresa, processata da uno o più algoritmi di riconoscimento facciale. Benché al momento tali software siano impiegati dalle forze di polizia unicamente come ausilio per orientare le indagini[3], risulta crescente la preoccupazione da parte di istanze politiche e scientifiche, associazioni per la tutela dei diritti e delle libertà civili. Come si avrà modo di approfondire meglio *infra* al capitolo II, da una parte l'Unione europea, tramite soprattutto la Commissione europea, e dall'altra, il Consiglio d'Europa, stanno segnalando ormai da qualche tempo i rischi legati all'impiego di tali strumenti di intelligenza artificiale, sia per l'elevata probabilità di sviluppo di risultati non attendibili, e dunque, di identificazioni errate, sia per la possibile strumentalizzazione a fini discriminatori e di controllo politico e sociale.

A questo punto, non è difficile immaginare che l'irruzione nel processo penale di un sapere scientifico in convulso divenire, continuerà ad arricchire l'elenco delle attività informali di polizia, anzi, sembrerebbe che i sistemi automatici di *facial recognition* stiano già traducendo il pronostico in realtà. La mutevolezza dello scenario presente e futuro in cui le investigazioni scientifiche dominano, impone allo studioso un approccio multidisciplinare che sia al riparo da soluzioni "preconfezionate" e allo stesso tempo verifichi con rigore la compatibilità delle suddette nuove tecniche con il principio di legalità processuale. Il principale obiettivo è quello della costituzione di tante regolamentazioni quanti sono i sistemi di riconoscimento biometrico più diffusi in ambito giudiziario, partendo dall'analisi degli snodi problematici che hanno in comune.

[3] Cfr. i capitoli III e IV per approfondirne le ragioni.

Ad ogni modo, non si può certamente negare la complessità del tema, sia dal punto di vista tecnico, sia per gli interessi in gioco. Infatti, a generare perplessità è l'introduzione di tali strumenti di indagine nel circuito dell'accertamento giudiziale prima di averne stabilito precise, uniformi e comuni condizioni di operatività. Come emerge già a partire da queste prime riflessioni, le tecniche automatizzate di riconoscimento, considerate nel loro intero "ciclo biometrico", risultano ancora ricche di insidie: il principale profilo di rilievo riguarda i requisiti di sicurezza, accuratezza, trasparenza e tracciabilità dei quali devono essere dotati tali sistemi anche e soprattutto quando vengono applicati algoritmi di riconoscimento automatico (cfr. *infra*, il capitolo II § 2).

Una volta presentate le caratteristiche fondamentali della disciplina e le principali questioni emergenti da quello che si può definire come cd. "*iter* biometrico", nel successivo capitolo II s'intende concentrare la ricerca sulla rappresentazione digitale e sul *template* inquadrandoli entro la categoria più ampia della "*digital evidence*": la presenza di determinati requisiti di robustezza e trasparenza, connessi a forme di intervento umano capaci di correggere l'esito scaturito dalla correlazione tra dati, oltre alla costante centralità dei diritti fondamentali (v. il capitolo III), saranno il presupposto inderogabile per l'affidabilità del prodotto di intelligenza artificiale.

1. *βίος* e *μέτρον*: una ricostruzione semantica

Al fine di poter avviare un'efficace analisi sulle questioni giuridiche emergenti dall'applicazione della scienza biometrica nel processo penale, occorre in primo luogo delimitarne il campo d'indagine attraverso una chiara comprensione del significato del termine e alcune precisazioni tecniche[4]. Tale operazione, di carattere ricostruttivo, non si presenta affatto scontata, essendo la scienza biometrica caratterizzata da una notevole complessità e interdisciplinarietà[5].

In primis, la biometria (dalle parole greche *βίος*=vita e *μέτρον*=conteggio o misura) può definirsi come la «disciplina che studia le grandezze biofisiche - sia fisiologiche, sia comportamentali - allo

[4] Il capitolo I è dedicato all'individuazione delle principali caratteristiche della disciplina biometrica e alla presentazione delle più diffuse tecniche di riconoscimento. Tale quadro teorico fornirà le coordinate dogmatiche necessarie per orientarsi all'interno della normativa nei successivi capitoli. Sia consentito il rinvio a E. Sacchetto, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Dir. Pen. Cont. – Riv. Trim.*, 2/2019, p. 467.

[5] «Se si vogliono comprendere appieno gli aspetti giuridici legati all'uso della biometria, quindi, non si può prescindere (…) dalla conoscenza, seppur minima, dei meccanismi di funzionamento delle tecniche biometriche». G. Bellomo, *Biometria e digitalizzazione della pubblica amministrazione*, in AA.VV., *A 150 anni dall'unificazione amministrativa italiana*, (a cura di) L. Ferrara, D. Sorace, Firenze University Press, Firenze, 2017, pp. 59 e ss. «Lo studio delle tecnologie biometriche implica conoscenze interdisciplinari che possono essere raccolte, in termini assolutamente generali, nella lista che segue: - elettronica; - informatica; - statistica; - medicina; - psicologia; - etica; - diritto». COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, 26.11.2010. Sul punto cfr. anche C. A. Jasserand, *Avoiding terminological confusion between the notions of 'biometrics' and 'biometric data': an investigation into the meanings of the terms from a European data protection and a scientific perspective*, in *International Data Privacy Law*, 2016, vol. 6, no. 1 e S. Girotto, *Biometria e nanomedicina: le nuove frontier della riconcettualizzazione tecnologica del corpo umano*, in *Nuova Giur. Civ.*, 2009, p. 9.

scopo di identificarne i meccanismi di funzionamento, di misurarne il valore e di indurre un comportamento desiderato in specifici sistemi tecnologici» (cd. "*biometry*")[6]. Essa consiste, dunque, in primo luogo, in una sistematizzazione della conoscenza, applicabile a ipotesi sperimentalmente controllabili, attraverso l'applicazione di alcune tecniche specifiche[7].

Prima di trovare ampia diffusione nel settore della sicurezza e dell'informatica[8], la disciplina biometrica è stata principalmente sfruttata per l'analisi di metodi matematici e statistici applicati alla biologia, alle scienze agrarie e forestali, alla medicina, alla genetica e alle scienze ambientali[9]. Tra le finalità principali di tale settore scientifico, rientrano lo studio della correlazione genetica tra le specie e le popolazioni, i dosaggi farmacologici, le diagnosi mediche e, infine, l'identificazione, nonché l'autenticazione degli individui[10].

---

[6] Cfr. "Biometria" o "*Biometry*", Enciclopedie *online* - Istituto dell'Enciclopedia italiana Treccani, http://www.treccani.it/enciclopedia/biometria/ (ultima visualizzazione il 19.2.2019), A.K. Jain, A. Ross, K, Nandakumar, *Introduction to biometrics: a textbook*, Springer, Berlin, 2011, pp. 1- 49, L. Cuomo, *Profili giuridici del trattamento biometrico dei dati*, in *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)*, fasc.1, 2014, p. 43, A. K. Jain, A. Ross, S. Prabhakar, *An Introduction to Biometric recognition*, in *IEEE Transactions on Circuits and Systems for Video Technology* 14(1):4 – 20, N. Nappi, *Iris recognition - I° part*, in *Proceedings of the conference during the International Summer School for Advanced Studies on Biometrics for Secure Authentication: biometrics, forensics and identity science for human-centered applications*, 7.06.2020, A. Monteleone, *Rilevazioni biometriche : lo stato della "privacy" delle "networked persons" tra il nuovo Codice ed i provvedimenti del Garante italiano*, in *Diritto&Diritti*, giugno 2004, p. 1, E. Mordini, C. Petrini, *Ethical and social implications of biometric identification technology*, in *Ann Ist Super Sanità*, 2007, vol. 43, no. 1, pp. 5-11, R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, A. W. Senior, *Guide to Biometrics*, Springer, New York, 2003. Il termine "biometria" è stato utilizzato per la prima volta nel 1901 nel primo numero di *Biometrika*, rivista scientifica di statistica fondata a Londra dalla Oxford University Press. Si v. F. Galton, Biometry, in *Biometrika*, vol. 1, 1, 1901, pp. 7-10.

[7] Cfr. *ex multis*, G. Preite, *Politica e biometria. Nuove prospettive filosofiche delle scienze sociali*, Tangram Edizioni Scientifiche, Trento, 2016, p. 21.

[8] A tal proposito, E. Mordini, *Il Volto e il Nome. Implicazioni Etiche, Sociali e Antropologiche delle Tecniche di Identificazione Biometriche*, in *MEDIC*, 2006, 14, p. 31, parla di «moderna biometria». G. Formici, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, in *Saggi - DPCE online*, 2019/2, p. 1109 afferma che «(…) molti datori di lavoro si propongono di utilizzare i dati biometrici per stabilire univocamente l'identità dei dipendenti presenti sul luogo di lavoro, mentre gli istituti bancari fanno sempre più uso di questi sistemi per individuare con certezza il soggetto avente accesso ad uno specifico luogo. Accanto a questi attori privati, tuttavia, anche le autorità pubbliche hanno preso consapevolezza dell'importanza del riconoscimento biometrico, sul versante della sicurezza pubblica o nazionale, delle indagini penali, della lotta al crimine, anche con finalità antiterroristiche o di controllo alle frontiere, oltre che per incrementare l'efficiente allocazione delle risorse e una corretta gestione dei servizi pubblici». Sul punto si veda anche R. Nunin, *Utilizzo dei dati biometrici da parte del datore di lavoro: la prescrizione del Garante per la privacy*, in *Il lavoro nella giurisprudenza*, 2007, 2, pp. 147 e ss.

[9] Sul punto si veda il sistema di Classificazione Decimale Dewey (CDD), di M. Dewey, in cui la "Biometria" è accorpata alla "Biostatistica" (CDD: 574.015195), classificata nella materia "Scienze naturali e Matematica" (CDD: 500), alla classe "Scienze della vita" (CDD: 574), per la sezione "Filosofia e teoria" (CDD:574.01), in L. Crocetti, D. Danesi (Eds.), *Classificazione decimale*, Dewey, Ed. n. 20, Vol. II, Roma, AIB, 1993. Si veda anche G. Montecchi, F. Venuda, *Manuale di biblioteconomia*, Milano, Editrice Bibliografica, 1999, pp. 124 e 243, K. Mather, *Elementi di biometria*, Boringheri, Torino, pp. 3 e ss., S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, Giappichelli, Torino, 2013, pp. 17 e ss.

[10] Invero, il campo di applicazione e di studio di tale scienza risulta estremamente vasto riguardando tutto ciò che è legato ad una qualche misurazione della vita: dalla biometria vegetale che consente per esempio di stabilire l'età di una specie botanica, alla biometria animale che classifica e analizza le caratteristiche principali degli animali, ovvero una biometria medica che costituisce la base conoscitiva dei principali esami clinici (per es. una TAC o una RMN).

Invero, da sempre gli esseri umani si servono di diverse caratteristiche del proprio corpo (come il volto o la voce) per interagire con altri individui e con il mondo circostante[11]. In particolare, con l'evoluzione dell'organizzazione della società è nata l'esigenza di riconoscere i soggetti e il corpo appare, da sempre, il più immediato mezzo di identificazione[12]. In seguito al crescente sviluppo tecnologico[13], l'utilizzo del corpo a fini identificativi si è diffuso soprattutto nel settore della sicurezza[14]. Con riferimento a quest'ultimo ambito di applicazione, l'*International Biometric Group*

[11] Cfr. S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, Giappicchelli, Torino, 2013, pp. 4 e ss., B. Lavanya, H. Hannah Inbarani, *A Survey of Biometric Techniques*, in *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, 7, 2015. «L'identificazione degli esseri umani è un'esigenza cognitivamente e psicologicamente fondamentale che si è manifestata senza eccezioni in ogni società», COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, cit.

[12] Per una prima panoramica sul tema cfr. S. Amato, F. Cristofari, S. Raciti, *Biometria: I codici a barre del corpo*, Giappichelli, Torino, 2013 e G. Preite, *Il riconoscimento biometrico - Sicurezza versus privacy*, Uni Service, Trento, 2007.

[13] Per i Paesi dell'Unione europea, gli anni novanta rappresentano il periodo di maggior sviluppo e sensibilizzazione sul tema. In particolare, notevole sviluppo ha avuto l'*Information and Communication Technology* (ICT) che costituisce l'insieme delle tecnologie che consentono di elaborare e comunicare l'informazione attraverso i mezzi digitali. Cfr. M. Kranzberg, *The Information Age: Evolution or Revolution?*, in B. R. Giulie, *Information Technologies and Social Transformation*, in *Nat. Academy Press*, London 1985, U. Pagallo, *Let Them Be Peers: The Future of P2P Systems and Their Impact on Contemporary Legal Networks*, in *European Journal of Legal Studies*, consultabile presso https://cadmus.eui.eu/handle/1814/15127 (visualizzato in data 2.1.2021).

[14] Di qui la nascita di due discipline quali l'antropometria e la dattiloscopia. L'antropometria può essere definita come la "madre" della moderna biometria. L'uso del termine è stato introdotto dall'antropologo e geografo Francis Bacon (Londra, 1561 – Londra, 1626) le cui ricerche furono indirizzate alla misurazione delle differenze individuali negli organismi viventi. Molte delle sue ricerche ed articoli scientifici furono volti a comprendere se le caratteristiche fisiche e mentali degli uomini variabili da persona a persona, dipendessero dalla sola eredità biologica o anche dalle condizioni ambientali di sviluppo e in quale misura. Successivamente, Francis Galton (Sparbrook, 1822 – Haslemere, 1911) ha approfondito più specificamente lo studio dei gemelli omozigoti e, analizzando le impronte digitali, ha misurato la probabilità che due individui diversi abbiano le medesime impronte, ne ha indagato l'ereditarietà e le caratteristiche in diversi gruppi razziali ideando un sistema per la loro classificazione. Il metodo di identificazione basato sulle impronte digitali è stato, poi, introdotto da William James Hershel (1860) ed il suo utilizzo in ambito criminale e giudiziario venne proposto da Henry Faulds (1880): sono state in seguito le ricerche di Galton e quelle svolte da Sir Edward Henry nello stesso periodo a impostare su base scientifica le applicazioni di tale metodo, favorendone l'adozione effettiva nelle aule giudiziarie. In seguito, Alphonse Bertillon (Parigi, 1853 – Parigi, 1914), un impiegato della prefettura della polizia di Parigi, ha ideato il primo sistema di classificazione fondato su misure di parti del corpo, che è stato definito metodo antropometrico o *bertillonage*. Il metodo era basato sullo studio antropometrico del capo (cefalometria e cefalosopia) e del corpo (somatometria e somatoscopia). Le caratteristiche generali del corpo venivano trascritte su una scheda e dal raffronto tra questa e il soggetto, si otteneva il riconoscimento. L'avvento della dattiloscopia (i cui primi studi possono farsi risalire intorno alla metà del 1700, cfr. *infra* il § 3.1) ha segnato il superamento del sistema del *bertillonage*. Ciò che ha comportato la crepa del *bertillonage* come strumento d'identificazione fu che alcune misure fisiche non fossero uniche. Nel 1903, infatti, nell'istituto penitenziario di Leavenworth nello Stato di Washington, mentre gli operatori procedevano all'identificazione di Will West, si resero conto che quel nome era già familiare e che anche le misure fisiche e le foto erano praticamente uguali a quelle di un altro detenuto William West schedato qualche tempo prima (M. Pulice, Sistemi di rilevazione di dati biometrici e privacy, in *Lavoro nella Giurisprudenza*, 2009, 10, 994, p. 2.). Nel momento in cui furono confrontate le impronte digitali, fu accertato che i due soggetti erano diversi. Il *bertillonage* dunque venne ritenuto meno convincente della proposta avanzata dal britannico Francis Galton di sfruttare le impronte digitali a fini investigativi. L'era del segnalamento dattiloscopico, oltre a rivoluzionare la storia dell'identificazione, ha avuto ripercussioni straordinarie sulla possibilità di rintracciare il reo dalle impronte lasciate sulla *scena criminis*. Fortissimo impulso allo studio e all'applicazione della disciplina biometrica in ambito di sicurezza, si è avuto con l'attacco terroristico alle torri gemelle di New York, l'11 settembre 2001. In particolare, «*in the immediate aftermath of 9/11, there was a clear shift in political priorities towards reasserted nationalism, the return to geopolitics, the hardening of state power and the closing of national borders*». S. Smyth, *Biometrics, surveillance and the law. Societies of restricted access, discipline and control*, Routledge, New York, 2019, p. 9. L'analisi dei più diffusi strumenti di riconoscimento biometrico verrà meglio approfondita *infra* i §§ 3 e ss. In ogni caso, sul piano di una generale ricostruzione storica, si segnala A. Giuliano, *Dieci e tutte diverse. Studio sui dermatoglifi*

(da qui in avanti IBG) ha precisato che il termine "*biometrics*" consiste nell'«uso automatizzato di caratteristiche fisiologiche o comportamentali per determinare o verificare l'identità» distinguendolo dalla nozione più generale di "*biometry*"[15]. Tale definizione è considerata un primo punto di riferimento nel settore informatico e della sicurezza: il ricorso all'aggettivo "*automated*" sembra specificare, in tal senso, un'imprescindibile caratteristica nella qualificazione di un sistema biometrico. Lo stesso documento dell'IBG ha poi precisato che un sistema biometrico include gli *hardware*, i *software* associati, i *firmware* e le componenti di *network* necessari per portare a termine il processo biometrico di registrazione e di comparazione[16].

Contestualmente, il *National Science and Technology Council* (da qui in avanti NSTC) e il sottocomitato sulla biometria hanno precisato, però, che "dato biometrico" consiste più precisamente nella «caratteristica biologica (anatomica e fisiologica) e/o comportamentale che può essere usata per ricognizioni automatizzate»[17].

Si tratta di due nozioni aventi un significato completamente differente, da cui è ragionevole desumere una disparità di vedute anche a livello istituzionale.

Al fine di giungere ad un'interpretazione condivisa della disciplina in esame, essenziale è stato il contributo del Consiglio d'Europa e dell'Unione europea, nel cui ambito più enti e istituzioni si sono interessati alle questioni emerse dal rapido diffondersi dell'impiego di sistemi biometrici sui quali si sono cominciate ad applicare sistematicamente tecniche di intelligenza artificiale (cfr. *infra* il capitolo II, § 2). Le prime fonti non sono riconducibili al diritto positivo, trattandosi principalmente di rapporti, raccomandazioni e linee guida. Esse hanno comunque assunto valenza per il prestigio dei centri di

---

umani, Torino, Tirrenia Stampatori, 2004, pp. 1 e ss., G. Iovane, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza*, Aracne editore, Roma, 2008, pp. 174 e ss., E. Mordini, C. Petrini, *Ethical and social implications of biometric identification technology*, in *Ann Ist Super Sanità* 2007, vol. 43, no. 1, pp. 5-11, e, con riferimento all'impatto del progresso scientifico sulla disciplina biometrica, v. A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross, J. L. Wayman, *Biometrics: A Grand Challenge*, in *Proceedings of International Conference on Pattern Recognition*, Cambridge, UK, 2004.

[15] L'INTERNATIONAL BIOMETRIC GROUP è una società internazionale che offre servizi nel settore della biometria sia nell'ambito pubblico che nell'ambito privato. Il termine "biometria" si riferisce a «*the automated use of physiological or behavioural characteristics to determine or verify identity*», INTERNATIONAL BIOMETRIC GROUP, *How is "biometrics" defined?*, in http://www.biometricgroup.com/public/reports/biometric/definition.htlm (visualizzato in data 10.1.2020). L'OECD (ORGANIZZAZIONE PER LA COOPERAZIONE E PER LO SVILUPPO ECONOMICO) - nel 2004 - ha fatto propria tale definizione nel documento WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-based technologies*, pp. 10 e 11; v. sul punto anche, S. Girotto, *Biometria e Nanomedicina*, cit., p. 2. Seguendo tale impostazione, i dati biometrici sono stati definiti anche come una «*digital representations of physiological features*», I. Van Der Plog, *Biometric identification technologies: ethical implications of the information of the body. Biometric Technology & Ethic*s, *BITE Policy* Paper, no. 1, 2005.

[16] V. INTERNATIONAL BIOMETRIC GROUP, *How is "biometrics" defined?*, cit. Nello stesso senso v. J. L.Wayman, *A Definition of "Biometrics"*, in *National Biometric Test Center Collected Works*, San Jose State University, 2000.

[17] Il NATIONAL SCIENCE TECHNOLOGY COUNCIL è un organo consultivo interno al governo federale degli Stati Uniti d'America. E' stato istituito il 23 novembre 1993 dal Presidente Bill Clinton con la specifica funzione di coordinamento della politica in ambito scientifico e tecnologico. Cfr. DEP. OF DEFENCE USA, *Report of the Defense Science Board Task Force on Defence Biometrics*, p. 8, D.C. 20301-2140, 2007: «*a measurable biological (anatomical and physiological) and/or behavioural characteristic that can be used for automated recognition*».

ricerca e delle istituzioni coinvolte, per l'apporto interdisciplinare di conoscenze fornito da una pluralità di esperti e come punto di partenza per i successivi interventi normativi (cfr. *infra*). A tal proposito si ricorda il "*Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*", del 2005, relativo all'applicazione ai dati biometrici della Convenzione 108 del 1981 del Consiglio d'Europa, sulla protezione degli individui riguardo al trattamento automatizzato di dati personali[18] che - più genericamente - considera la biometria come «*a traditional method of identification of individuals: fingerprints for instance have been used for decades*»[19]. Quasi contestualmente il *Joint Research Center*, servizio scientifico della Commissione europea, ha condotto uno studio sulle implicazioni etiche e giuridiche derivanti dal trattamento dei dati biometrici, definendo questi ultimi come «*any human physical or biological feature that can be measured and used for the purpose of automated or semi-automated identification*»[20].

Nel contesto italiano, una prima definizione - valorizzata in dottrina[21] - della disciplina è stata fornita dal Comitato nazionale per la bioetica, che ha individuato la "biometria" come una nuova tecnica «di identificazione o "misurazione" dell'essere umano attraverso la rilevazione di determinate caratteristiche fisiche e comportamentali che vengono tradotte in sequenze matematiche e conservate in banche dati elettroniche»[22].

---

[18] COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE 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*, in https://rm.coe.int/16806840ba, February 2005. Giova ricordare che la Convenzione 108 del 1981 (*Convention for the protection of individuals with regard to automatic processing of personal data*), anche a seguito dell'introduzione del protocollo di aggiornamento nel 2018 (Convenzione 108+), ha dato attuazione all'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950, definendo i principi per la tutela della vita privata delle persone. Il report ha avuto la funzione di guida, contribuendo al dibattito circa la relazione tra diritti umani e biometria. Per il protocollo di aggiornamento del 2018 v. https://www.privacy.it/2018/05/18/convenzione-108-aggiornamento-2018/ (ultimo accesso in data 26.1.2021).

[19] COUNCIL OF EUROPE, *Consultative Committee 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*, cit., p. 2.

[20] EUROPEAN COMMISSION, *Biometrics at the Frontiers: assessing the impact on society. For the European Parliament Committee on Citizen's Freedom and Rights, Justice and Home Affaire (LIBE)*, in file:///C:/Users/ernestina/Downloads/gp_eudor_WEB_LFNA21585ENC_002.pdf.en.pdf (ultimo accesso in data 25.11.2020). In linea con questa definizione A. K. Jain, A. A. Ross, K. Nandakumar, *Introduction to biometrics*, Springer Science & Business Media, 2011, pp. 2-3.

[21] Cfr. S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, cit.

[22] COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria,* cit., p. 3. Precedentemente, un riferimento alla biometria si rinviene nell'art. 1, lett. *g*), d.p.r. n. 513/1997 ("*Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici*") che, nel qualificare giuridicamente il documento informatico e la firma digitale, ha definito "chiave biometrica" la « sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità digitale basati su specifiche caratteristiche fisiche dell'utente». Successivamente, l'art. 8, comma 3, del d.P.R. n. 445 del 2000 ha ridefinito le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico anche con riferimento all'eventuale uso di chiavi biometriche. Con il d.lgs. 30.6.2003 n. 196 il legislatore ha riconosciuto la rilevanza dei dati biometrici come una particolare tipologia di informazioni personali per la quale è previsto l'obbligo della notifica all'Autorità Garante (art. 37, comma 1, lett. *a*) per la natura del trattamento ritenuto più delicato rispetto ad altri, senza, peraltro, mai fornire una puntuale definizione.

E' evidente che si tratta di accezioni tutte differenti, specchio di un divario terminologico sia nella letteratura scientifica sia, come poc'anzi accennato con riferimento al contesto internazionale, a livello istituzionale[23]. E, benché si ritenga "fisiologica" l'esistenza di sfumature semantiche in considerazione delle differenti qualificazioni di una determinata disciplina, a seconda dell'ambito di applicazione, non risulta ancora del tutto univoco in dottrina a quale nozione si possa ricorrere nell'approccio giuridico allo studio della materia[24].

L'*International Standard Organization* (ISO/IEC 2382–37) ha, perciò, operato un primo tentativo di sistematizzazione da un punto di vista tecnico di tutte le definizioni fornite - nei diversi ambiti - al fine di armonizzare da un punto di vista tassonomico la materia[25]. In particolare, per "dato biometrico" s'intende «*[the] biological or behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition*». E' definito "*biometric recognition*", invece, «[the] *recognition of individuals based on their biological and behavioural characteristics, encompassing biometric verification and biometric identification*». Permane invece il riferimento all'aggettivo "*automated*" nella definizione di «*biometrics*»[26]: nella categoria di "dato biometrico" è ricondotto tanto il dato grezzo, proveniente da un determinato soggetto (sia esso fisico, fisiologico o comportamentale), quanto le immagini digitalizzate e i modelli

[23] A tal proposito, nello studio di C. A. Jasserand si evidenzia che «(…) *different European bodies have indeed used the term 'biometrics' in their legal opinions and reports to mean all at the same time 'biometric data', 'identification method', and 'biometric technologies'*. (…) *Several bodies belonging to the Council of Europe's level have used the term 'biometrics' as synonyms of 'biometric technologies' or 'biometric systems' in the specific context of personal data and in the broader context of human rights*». C. A. Jasserand, *Avoiding terminological confusion between the notions of 'biometrics' and 'biometric data': an investigation into the meanings of the terms from a European data protection and a scientific perspective*, in *International Data Privacy Law*, 2016, vol. 6, no. 1. Sul punto v. anche la ricostruzione semantica della definizione di E. J. Kindt, *Having yes, using no? About the new legal regime for biometric data*, in *Computer Law and Security Review*, 34, 2018, p. 14.

[24] «La difficoltà nell'individuazione di una convenzione definitoria è dovuta sia al fatto che manca nel panorama giuridico attuale una qualificazione normativa condivisa di tali categorie di dati, sia al fatto che il progresso della ricerca scientifica e l'evoluzione della tecnologica ampliano continuamente le possibilità di acquisizione e di elaborazione di questi dati vanificando ogni tentativo di fornire un'immagine statica della categoria». A. Iannuzzi, F. Filosa, *Il trattamento dei dati genetici e biometrici*, in *Dirittifondamentali.it*, fasc. 2/2019.

[25] INFORMATION TECHNOLOGY – VOCABULARY – Part 37: *Biometrics*, reperibile all'indirizzo https://www.iso.org/committee/313770.html (ultimo accesso in data 25.11.2020), oggetto di una recente revisione con la pubblicazione delle disposizioni ISO/IEC 19795-1:2021, IDT reperibili all'indirizzo https://www.iso.org/standard/73515.html (visualizzato in data 2.10.2021). Le definizioni contenute nel testo ISO sono state altresì riprese nel 2014 dall'autorità italiana Garante per la protezione dei dati personali nelle *Guidelines on Biometric Recognition and Graphometric Signature*, Annex A to the Garante's Order of 12 November 2014, 3, http://194.242.234.211/documents/10160/0/ GUIDELINES+ON+BIOMETRIC+RECOGNITION (ultimo accesso in data 15.11.2020). Cfr. J. Wayman, R. McIver, P. Waggett, S. Clarke, M. Mizoguchi, C. Busch, N. Delvaux, A. Zudenkov, *Vocabulary harmonisation for biometrics: the development of ISO/IEC 2382 Part 37* in *The Institution of Engineering and Technology*, Vol. 3, 1, 2014, pp. 1-8, in particolare con riferimento allo sforzo decennale da parte del "Comitato per gli standard" dell'INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - INTERNATIONAL ELECTROTECHNICAL COMMISSION JOINT TECHNICAL COMMITTEE (ISO / IEC JTC1 SC37) per creare un vocabolario sistematico per la disciplina biometrica.

[26] Definita come «*automated recognition of individuals based on their behavioural and biological characteristics*». Cfr. ISO/IEC JTC12382-37:2012 e E. Micheli Tzanakou, K.N. Plataniotis, *Biometrics: Terms and Definitions*, in AA.VV., *Encyclopedia of Cryptography and Security*, (a cura di) H.C.A. Van Tilborg, S. Jajodia, Springer, Boston, 2011.

elettronici che permettono l'identificazione, l'autenticazione o la verifica automatica dell'identità. Di conseguenza, e in conformità con la norma internazionale ISO/IEC 2382-37, "biometria" come sostantivo dovrebbe essere usato solo per significare il "riconoscimento automatizzato".

L'accezione di "dato biometrico" è stata posta invece alla base del parere 3/2012 del Gruppo di lavoro WP2914[27], che ha identificato i dati biometrici come quelli ricavati da «proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche o azioni sono tanto proprie di un certo individuo in quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità»: la stessa nozione è stata ripresa a sua volta dall'Autorità Garante per la protezione dei dati personali nelle "*Linee guida in materia di riconoscimento biometrico e firma grafometrica*"[28] ove si è considerata "caratteristica biometrica", la qualità «biologica o comportamentale di un individuo da cui possono essere estratti in modo ripetibile dei tratti biometrici (*biometric features*) distintivi e idonei al riconoscimento biometrico»[29].

Quasi contestualmente, il Consiglio d'Europa nel documento "*Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*" nel definire "dato biometrico" non sembra più assumere una posizione netta (v. *supra*), affermando che: «*biometric data (or biometrics) are measurable, physiological or behavioural characteristics that can be used to determine or verify identity. Biometrics is also defined as 'the automated use of physiological or behavioural characteristics to determine or verify individuals'*»[30].

Successivamente, con l'entrata in vigore del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio (da qui in avanti GDPR), è stata finalmente introdotta una definizione normativa che sembra aver tenuto in considerazione la maggioranza dei tratti tipici della particolare categoria di dati descritti finora, ma che non risulta priva di incertezze interpretative[31]. L'art. 4(14) ha definito, infatti,

---

[27] Cfr. C. A. Jasserand, *Avoiding terminological confusion between the notions of 'biometrics' and 'biometric data': an investigation into the meanings of the terms from a European data protection and a scientific perspective*, in *International Data Privacy Law*, 2016, vol. 6, no. 1, p. 64, ove l'Autrice afferma che: « (…) *although the current version of the Standard is the first one published and might be subject to revision, it has already been quoted as a document of reference by national data protection authorities*», riferendosi proprio al Garante (*Italian Data Protection Authority*), *Guidelines on Biometric Recognition and Graphometric Signature*, Annex A to the Garante's Order of 12 November 2014.

[28] AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in materia di riconoscimento biometrico e firma grafometrica*, allegato A al Provvedimento del Garante del 12 novembre 2014, reperibile in www.gpdp.it (visualizzato in data 30.11.2020).

[29] AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida*, cit., p. 4.

[30] COUNCIL OF EUROPE, *Progress report on the application of the principles of convention 108 to the collection and processing of biometric data*, 2013, in https://rm.coe.int/progress-report-on-the-application-of-the-principles-of-convention-108/1680744d81, (ultimo accesso in data 25.11.2020).

[31] 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). Il d.lgs. 101, 10.8.2018, contenente le disposizioni per l'adeguamento della normativa nazionale ai principi del regolamento (UE) 2016/679, ha avuto la funzione di armonizzare le norme enunciate dal nostro

"biometrici" «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»[32]. L'enunciazione

legislatore nel codice in materia di protezione dei dati personali (d.lgs. 196/2003) con quelle introdotte dal regolamento. Il regolamento ha abrogato le precedenti disposizioni contenute nella direttiva 95/46/CE (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 di tali dati - GU l. 281 del 23.11.1995). Quest'ultima, conosciuta anche come "direttiva madre", non riconosceva la specificità dei dati biometrici e li faceva, perciò, rientrare nella generale categoria dei dati personali, che ricomprendeva «*qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identicazione o ad uno o più elementi o specifiche caratteristiche della sua identità fisica, fisiologica, psichica, economica, culturale o sociale*». In tale prospettiva, la direttiva 95/46/CE, per dare risalto alla "sensibilità" della tipologia dei dati personali in esame, prevedeva delle prescrizioni specifiche mirate a garantire un livello di protezione più elevato. In particolare, a norma dell'art. 29 della direttiva 95/45/CE, era stato istituito il "Gruppo per la tutela dei dati personali" ossia un organo consultivo indipendente dell'Unione Europea avente competenze in materia di tutela dei dati e della vita privata. Più nel dettaglio, si deve a tale ente il merito di aver elaborato un documento di riferimento nel settore, il *Documento di lavoro sulla biometria*, nel quale sono stati specificati alcuni principi basilari aventi ad oggetto la natura dei dati biometrici e le modalità di trattamento (GRUPPO PER LA TUTELA DEI DATI PERSONALI – ARTICOLO 29, *Documento di lavoro sulla biometria*, 1° agosto 2003, in https://www.garanteprivacy.it/documents/10160/10704/443868.pdf/f6caf8cd-dcd3-426f-b64d-388a9863391a?version=1.0, ultimo accesso in data 25.11.2020). Tale documento ha specificato che con "sistemi biometrici" si vuole indicare le applicazioni di tecnologie biometriche che permettono l'identificazione e/o l'autenticazione/verifica automatica di un individuo. Il d.lgs. n. 196/2003, recante "Codice in materia di protezione dei dati personali" (d'ora in avanti anche codice *privacy*), recependo le indicazioni dettate dalla direttiva, all'interno di un *corpus* normativo ora abrogato, aveva costruito una efficace cornice normativa per il trattamento dei dati genetici e biometrici, innanzitutto considerando l'informativa e il consenso. Il trattamento dei dati genetici e dei campioni biologici poteva avvenire solo previo consenso informato dell'interessato. Inoltre, l'art. 90 del codice *privacy*, abrogato dal d.lgs. 101/2018, prevedeva che il trattamento dei dati genetici potesse realizzarsi successivamente al rilascio di una apposita autorizzazione del Garante per la protezione dei dati personali, sentito il Ministro della salute, che acquisiva, a tal fine, il parere del Consiglio superiore di sanità. Per un'efficace ricostruzione sul punto, si v. A. Iannuzzi, F. Filosa, *Il trattamento dei dati genetici e biometrici*, in *Dirittifondamentali.it*, fasc. 2/2019, P. De Hert, *Biometrics: legal issues and implications*, in *Background paper for the Institute of Prospective Technological Studies*, DG JRC – Sevilla, European Commission, January 2005 e F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza artificiale*, in AA.VV., *Intelligenza artificiale, protezione dei dati personali e regolazione*, (a cura di) F. Pizzetti, Giappichelli, Torino, 2018, pp. 5 e ss. In linea con succitata confusione interpretativa della definizione di "dato biometrico" cfr. EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Person identification, human rights and ethical principles. Rethinking biometrics in the era of artificial intelligence*, 2021, p. 4, reperibile all'indirizzo https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)697191 (visualizzato in data 30.1.2022).

[32] L'accezione è stata fatta propria anche dalla direttiva 2016/680/UE del Parlamento europeo e del Consiglio del 27.4.2016, relativa alla 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, nonché alla libera circolazione di tali dati e dal d.lgs. 10.8.2018, n. 101 (cfr. il § che segue). Anche il regolamento (UE) 2018/1725, art. 3 (18), ha abbracciato la medesima definizione di "dato biometrico". Analogamente, la stessa nozione è richiamata dalla proposta di regolamento «*on a European approach for Artificial Intelligence*», COM(2021) 206 final (cfr. il capitolo II § 2.2.1): «'*biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*». Giova ricordare la recente proposta di integrazione della definizione di "dato biometrico", da parte del *Committee on the Internal Market and Consumer Protection Committee on Civil Liberties, Justice and Home Affairs* (EUROPEAN PARLIAMENT), con la nozione di "*biometrics-based data*" ossia «*data resulting from specific technical processing relating to physical, physiological or behavioural signals of a natural person, such as facial expressions, movements, pulse frequency, voice, key strikes or gait, which may or may not allow or confirm the unique identification of a natural person*» (cfr. *Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts* (COM2021/0206 – C9-0146/2021 – 2021/0106(COD)), 20.4.2022).
L'art. 9 § 1 GDPR stabilisce poi il divieto generalizzato di trattamento dei dati genetici e biometrici, a meno che non sia stato rilasciato il consenso. Il trattamento è lecito, invece, per finalità lavorative e previdenziali, qualora sia necessario tutelare un interesse vitale, per il raggiungimento delle finalità di legittime attività di fondazioni, associazioni o altri organismi senza scopo

suggerisce che, per essere considerati "biometrici", i dati personali devono soddisfare una serie di criteri[33]. Innanzitutto devono costituire "dati relativi a una persona fisica identificata o identificabile". L'interpretazione di questo requisito risulta piuttosto intuitiva e non comporta particolari problematiche.

Il secondo criterio appare invece molto più controverso poichè il GDPR non chiarisce esplicitamente come debba essere interpretata l'espressione "trattamento tecnico specifico". In tal senso, il considerando 51 del GDPR afferma che «il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica»[34]. Si osserva non solo un mutamento da "trattamento tecnico specifico" a "dispositivo tecnico specifico", ma cambia anche la finalità: da quella di "consentire" o "confermare" l'"identificazione univoca", all' "identificazione" o l' "autenticazione" di una persona fisica. Il tema risulta attualmente al centro di un ampio dibattito scientifico[35]. L'interpretazione maggioritaria al momento riconosce come "*specific technical processing*" il procedimento di conversione di un campione grezzo nella sua rappresentazione digitale (cd. "*biometric sample*") ovvero nel corrispondente *template* biometrico[36], ossia, come si vedrà meglio *infra*[37], il modello elettronico delle caratteristiche fondamentali di un dato tratto biometrico. Questo perché solo tale operazione consentirebbe «l'identificazione univoca o l'autenticazione di una persona fisica». Tuttavia, si ritiene del tutto ragionevole far rientrare in tale categoria qualsiasi operazione svolta su questi particolari dati personali con o senza l'ausilio di strumenti elettronici, che riguarda la raccolta dei dati, la registrazione, l'organizzazione, la conservazione, l'elaborazione, l'estrazione e il raffronto dei dati biometrici degli interessati. Ciò in ragione del fatto che la conservazione e

di lucro, qualora i dati personali particolari siano resi manifestamente pubblici dall'interessato, per lo svolgimento di attività difensive ed investigative, oppure per il raggiungimento di un interesse pubblico rilevante o per un interesse pubblico rilevante riguardante il sistema sanitario nazionale e regionale ed infine per scopi statistici o scientifici, così come precisamente disciplinato dall'art. 89.

[33] Cfr. C. Jasserand, *Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data*, in *European Data Protection Law Review* 2, no. 3, 2016, pp. 297–311.

[34] Il contenuto del considerando non è presente nella direttiva 2016/680/UE.

[35] Cfr. E. J. Kindt, *Having yes, using no? About the new legal regime for biometric data*, in *Computer Law and Security Review*, 34, 2018 che dà conto di tale dibattito in letteratura.

[36] Le *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video* pubblicate dall'*European Data Protection Board* il 29.1.2020 parlano più generalmente di "misurazioni" (il § 74 specifica che «per poter configurare un trattamento di dati biometrici, secondo la definizione del GDPR, il trattamento di dati grezzi, come ad esempio le caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, deve comprendere una misurazione di tali caratteristiche. Poiché i dati biometrici sono il risultato di dette misurazioni, il GDPR afferma nel suo articolo 4, paragrafo 14, che sono dati "[…] ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca […]"»). Il testo è reperibile all'indirizzo https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_it.pdf (visualizzato in data 13.1.2022).

[37] Cfr. il § 2.2 per la differenza intercorrente fra "*biometric sample*" e "*biometric template*".

l'archiviazione di un dato biometrico, pur non avendo come obiettivo diretto l'identificazione o l'autenticazione di una persona, costituiscono evidentemente precondizioni alle suddette finalità[38].

Il terzo criterio riguarda le qualità intrinseche degli interessati. Queste possono essere fisiche, fisiologiche o comportamentali e sono diverse dalle qualità accidentali, come per esempio l'indirizzo di residenza della persona interessata, la sua posizione lavorativa in un determinato momento storico, i dati sull'occupazione, ecc. Le tre caratteristiche possono essere utilizzate anche per identificare le diverse categorie di dati biometrici (cfr. *infra* il § 1.1).

Il quarto e ultimo criterio fornito dal GDPR è logicamente collegato al primo e rappresenta il punto di rottura con la definizione adottata, invece, a livello internazionale dall'*International Standard* ISO/IEC 2382–37 (cfr. *supra*). I dati biometrici, infatti, non necessariamente permettono l'identificazione univoca degli individui di per sé, come sottolineato anche dall'Autorità europea di controllo per la protezione dei dati[39]. Tuttavia, per essere considerati come "dati personali", ai sensi del GDPR, essi devono consentire o confermare univocamente l'identità di una persona fisica[40]. Invero, mentre da un punto di vista giuridico identificare univocamente un individuo significa

[38] Rimane il fatto che «*biometric characteristics are not themselves considered biometric data. Only the personal data "resulting" from their processing qualify as biometric data. Thus, it is not the face of an individual, but the images of their face (pictures) that would be classified as biometric data. Likewise, it is not their fingertip, but a fingerprint image that will be classified as biometric data. As legally defined, "biometric data" are first of all "personal data". To be protected under data protection rules, personal data need to be, at least, part of a "filing system"or processed by automatic means. The biometric characteristics themselves cannot be processed. Only the data generated from these characteristics can*». Cfr. *Towards the European Level Exchange of Facial Images Legal Analysis for TELEFI project*, 7.2.2020, reperibile su https://www.telefi-project.eu/sites/default/files/TELEFI_LegalAnalysis.pdf, (visualizzato in data 22.9.2021). Cfr. anche E. J. Kindt, *Having yes, using no? About the new legal regime for biometric data*, cit., p. 11, «*a database with facial images or fingerprints without biometric processing would hence not be considered a database with biometric data or a biometric database. We contend however that precisely such databases are the pre-condition and allow for biometric identification, as explained above, and such databases are therefore a risk for the fundamental rights and freedoms of the data subjects. Therefore, the 'fitness' of data to be used by automated means for identification or identity verification purposes should in our view rather be taken into account when developing a legal protective framework for the use of biometric data. This would be – what we call – an objective approach. The mere collecting and storing of facial images, fingerprints or iris images, is by the legislator hence not considered as biometric data or processing biometric data. Facial images only become biometric data under the GDPR and the Directive (EU) 2016/680 if they are used for biometric comparison, and more precisely, if they are the result of 'specific technical processing'. This is what we understand from the new legal definition*». Cfr. anche C. Jasserand-Breeman, *Reprocessing of biometric data for law enforcement purposes: Individuals' safeguards caught at the Interface between GDPR and the "Police" directive?. Groningen, University of Groningen*, reperibile su https://research.rug.nl/en/publications/reprocessing-of-biometric-data-for-law-enforcement-purposes-indiv (visualizzato in data 22.9.2021).

[39] EUROPEAN DATA PROTECTION SUPERVISOR, *14 misunderstandings with regard to Biometric Identification and Authentication*, p. 3.

[40] Tra l'altro, seguendo tale definizione non rientrerebbero i dati utilizzati per finalità di categorizzazione (cfr. *infra* il § 2.4). A tal proposito, cfr. E. J. Kindt, *Having yes, using no? About the new legal regime for biometric data*, cit., p. 12, «*governmental databases, collecting and keeping images of faces or fingerprints, for example collected for eID cards, do hence not fall under any specific biometric legislation if not used for identification purposes, other than the general data protection rules, as for all other personal data. There are hence no major restrictions or specific protection for such data collections. However, at the same time, such collections remain vulnerable for re-use, including biometric comparison and use for identification purposes*».

tecnicamente stabilire l'identità di una persona[41] - e, in questo senso, la definizione sopra richiamata potrebbe logicamente "reggere" - dal punto di vista scientifico-forense risulta invece del tutto errato definire il risultato di una comparazione biometrica come un'identificazione univoca. La definizione presente nel GDPR e nella direttiva 2016/680/UE non avrebbe riscontro scientifico[42]: sarebbe molto più opportuno esprimersi in termini di probabilità di riconoscimento, o meglio sarebbe più coerente riformulare la definizione come «*personal data relating to the physical, physiological or behavioural characteriscs which can be used to recognize individuals to a certain degree of probability*»[43]. A differenza di altri elementi identificativi, i dati biometrici, quando impiegati, non restituiscono mai un'identificazione certa e univoca. Più realisticamente, la comparazione di dati biometrici permette il riconoscimento di individui con un certo grado di probabilità. Essi sono il frutto di un procedimento di generalizzazione di risultati ottenuti attraverso una rilevazione parziale per campioni dell'intera popolazione da cui è stato estratto il tratto considerato. La disciplina statistica considera il risultato di compatibilità come una mera inferenza (cfr. il capitolo III, § 1.3). Pertanto, secondo una visione consolidata, i dati biometrici dovrebbero essere considerati come tali «*even if patterns used in practice to technically measure them involve a certain degree of probability*»[44]. Sulla base di queste premesse si potrebbe proporre una nuova definizione di "dato biometrico", da intendersi come dato personale riferibile direttamente o indirettamente a caratteristiche biologiche o comportamentali uniche o distintive di esseri umani, impiegabile - tramite mezzi automatizzati - a fini di riconoscimento dell'identità di una persona fisica vivente. Si ritiene che la definizione contenuta nei succitati documenti normativi europei sia in un certo senso pericolosa e fuorviante dal momento che, per i motivi esposti poc'anzi, rispetto a determinate espressioni ivi impiegate non rispecchierebbe la realtà da un punto di vista tecnico[45].

---

[41] Per esempio, l'articolo 66 c.p.p. dispone che nel primo atto in cui è presente l'imputato, esso dichiari «le proprie generalità e quant'altro può valere a identificarlo». Inoltre, come si vedrà meglio *infra* al § 2, l'articolo 349 c.p.p. precisa poi che la polizia giudiziaria procede alla identificazione della persona nei cui confronti vengono svolte le indagini e delle persone in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti, anche eseguendo, ove occorra, rilievi dattiloscopici, fotografici e antropometrici nonché altri accertamenti.

[42] Cfr. S. Stalla Bourdillon, *The GDPR and The Biggest Mess of All: Why Accurate Legal Definitions Really Matter*…, 12.4.2016, reperibile all'indirizzo https://peepbeep.wordpress.com/2016/04/12/the-gdpr-and-the-biggest-mess-of-all-why-accurate-legal-definitions-really-matter/ (visualizzato in data 7.10.2021).

[43] Cfr. *supra*, la definizione ISO/IEC 2382–37.

[44] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 4/2007 on the concept of personal data*, 2007, p. 8.

[45] Si anticipa che, come si vedrà meglio *infra*, il Consiglio dell'Unione europea nel primo testo di modifica delle disposizioni contenute nella proposta di regolamento sull'intelligenza artificiale (AI ACT, COM(2021) 206 final, reperibile all'indirizzo https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence), ha richiesto che fosse eliminata l'espressione «*which allow or confirm the unique identification of that natural person*». Cfr. *infra* il capitolo II, § 2.1. Il Parlamento europeo, tramite il COMMITTEE ON LEGAL AFFAIRS FOR THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION AND THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft Opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts* (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 2.3.2022 ha successivamente proposto di emendare la definizione come segue «*personal data resulting from specific technical processing*

In seguito a tale ricostruzione sinottica, risulta ragionevole intendere il "dato biometrico", sia come campione proveniente da un individuo[46], sia come immagine digitalizzata (cd. "*biometric sample*") o come "modello biometrico" o "*template*", in qualità di dato fisico, fisiologico o comportamentale convertito in un codice identificativo, tutti sottoposti a specifici trattamenti tecnici, finalizzati ad eseguire comparazioni volte, *inter alia*, al riconoscimento[47].

1.1. Il trattamento dei dati biometrici e la direttiva 2016/680/UE

La definizione di "dato biometrico" introdotta dal regolamento (UE) 2016/679 (cd. GDPR) consente di soffermarsi brevemente su alcuni dei principi fondamentali, sanciti nella già menzionata direttiva 2016/680/UE del Parlamento europeo e del Consiglio, datata 27 aprile 2016, "relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati" (cd. LED), utile per una più approfondita analisi che seguirà successivamente[48]. È lo stesso art. 2 del GDPR a esplicitare l'ambito di applicazione materiale del regolamento, escludendo il trattamento 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» (art. 2, par. 2, lett. *d*). In linea con tale disposizione risultano altresì il considerando n. 19 GDPR, che prevede che il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di

relating to the physical, or physiological or behavioural characteristics of a natural person, which confirm the unique identification of that natural person, such as dactyloscopic data».

[46] Come si vedrà meglio *infra*, esso può essere prelevato coattivamente, oppure reperito senza esercitare alcun tipo di coercizione fisica o morale sulla persona.

[47] In questo senso, cfr. S. Girotto, *Biometria e nanomedicina: le nuove frontiere della riconcettualizzazione tecnologica del corpo umano*, in *Nuova Giur. Civ.*, 2009, 9, p. 20452, Y. Liu, *Identifying Legal Concerns in the Biometric Context*, in *Journal of International Commercial Law and Technology* Vol. 3, 1, 2008 in cui l'autore afferma che: «*the legal significance of biometric data*» include «*raw biometric images and biometric templates*», A. I. Awad, A. E. Hassanien, *Impact of Some Biometric Modalities on Forensic Science*, in AA.VV., *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications*, (a cura di) A.K. Muda et al., in *Studies in Computational Intelligence* 555. S. Smyth, nella sua recente ricerca "*Biometrics, surveillance and the law. Societies of restricted access, discipline and control*", Routledge, New York, 2019, p. 21, afferma che «*The term biometrics refers to the measurement of physical features of the human body. Put differently, biometrics is [also] the science of automatic identification or identity verification of individuals using [unique] physiological or behavioural characteristics*». Per completezza, si veda anche M. Smith, M. Mann, G. Urbas, *Biometrics, Crime and Security*, Routledge, New York, 2018, p. 2 e J. R. Vacca, *Biometric Technologies and Verification Systems*, Butterworth-Heinemann, Burlington, 2007.

[48] Da qui in avanti "LED", ossia "*Law Enforcement Directive*", cfr. *supra* la nota n. 32. Con il presente paragrafo s'intendono richiamare brevemente i principi fondamentali per il trattamento del dato biometrico a fini di prevenzione e repressione del reato; seguirà nel capitolo II una ricostruzione della nozione di dato biometrico digitalizzato e di *template* entro alcune delle categorie dogmatiche processuali tradizionali. Tale sforzo classificatorio sarà utile per l'analisi del trattamento del dato biometrico digitalizzato nello spettro delle garanzie processuali fondamentali (v. il capitolo III).

sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica, e la libera circolazione di tali dati siano oggetto di uno specifico atto dell'Unione, ossia la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, e il considerando n. 11 della LED, il quale specifica la *ratio* della direttiva, ossia l'introduzione di norme specifiche relative alla 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, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, nel rispetto della natura specifica di tali attività. Le autorità competenti possono includere, prosegue il considerando n. 11, «non solo autorità pubbliche quali le autorità giudiziarie, la polizia o altre autorità incaricate dell'applicazione della legge, ma anche qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici (…). Qualora tale organismo o entità trattino dati personali per finalità diverse da quelle della presente direttiva, si applica il regolamento (UE) 2016/679 (…)».

La direttiva costituisce pertanto una *lex specialis* rispetto al GDPR: in particolare, la disciplina ivi contenuta racchiude un inevitabile bilanciamento tra l'interesse del singolo alla tutela dei dati personali e le esigenze di sicurezza sociale e, più in generale, di natura pubblicistica connesse alla tutela dell'ordine pubblico e alla cooperazione tra le diverse autorità di pubblica sicurezza[49]. A livello interno, il quadro normativo si completa con il d.lgs. 18.5.2018, n. 51, attuativo delle misure sovranazionali, che recepisce pressoché integralmente la direttiva, riportando gli stessi contenuti[50].

[49] Cfr. *ex multis* B. Galgani, *Giudizio penale, habeas data e garanzie fondamentali*, in *Arch. pen*., 1/2019, pp. 3 e ss., A. Ricci, *Il trattamento dei dati personali per finalità di prevenzione, indagine, accertamento e perseguimento dei reati. Riflessioni sul d.lgs. 18 maggio 2018, n. 51, di attuazione della dir. 2016/680/UE*, in *Nuove Leggi Civ. Comm.*, 2019, 3, p. 572, P. Troisi, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, in AA.VV., *La nuova disciplina europea della privacy*, (a cura di) S. Sica, V. D'Antonio, G. M. Riccio, Giuffrè, Milano, 2016, pp. 313 e ss., S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, pp. 87 e ss., A. Fonsi, *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time*, in *Penale Diritto e Procedura*, 13.5.2021, p. 4.

[50] Giova ricordare che, seppur in via transitoria, risultano attualmente in vigore la normativa attuativa di rango regolamentare di cui al d.P.R. 15.1.2018, n. 15 e il decreto del Ministero dell'Interno 24.5.2017, entrambi non completamente aderenti al contenuto della LED e del d.lgs. 51/2018. Infatti, l'art. 57 d.lgs. 196/2003 aveva previsto l'introduzione di un d.P.R. per l'adozione della normativa attuativa sul trattamento dei dati a fini di polizia di cui all'art. 53 dello stesso d.lgs. 196/2003. Il d.P.R. è stato introdotto il 15.1.2018. L'art. 57 è stato poi abrogato per effetto dell'attuazione della LED. L'art. 49, c. 3 del d.lgs. 51/2018 ha disposto che, in via transitoria, il d.P.R. rimanga in vigore fino all'adozione di una differente disciplina attuativa del d.lgs n. 51/2018 stesso. Pertanto, il d.P.R. deve considerarsi abrogato nella misura in cui non sia più compatibile con il d.lgs. 51. Per quanto concerne invece il d.m. 24.5.2017, esso era stato adottato in attuazione dell'allora vigente art. 53 c. 3 del codice della privacy per regolare i "trattamenti non occasionali" posti in essere dal "Centro elaborazione dati del Dipartimento della pubblica sicurezza o da forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento" e oggi rimane transitoriamente in vigore seppur parzialmente superato dalla normativa contenuta nel GDPR e nella LED. Le previsioni transitoriamente in vigore concernono esemplificativamente il diritto di accesso, rettifica e integrazione dell'interessato (artt. 9 e 10), l'informativa da rendere (art. 13), il limite dello svolgimento del trattamento per fini istituzionali (art. 18), la disciplina sul trasferimento dei dati all'estero (art. 42). Su questo punto v. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, p. 134.

Ai fini della presente trattazione si deve tenere in conto che, seppure le finalità della direttiva siano quelle di prevenzione, indagine, repressione dei reati ed esecuzione di sanzioni penali, diverse sue disposizioni richiamano quelle contenute nel GDPR, avente ad oggetto - come visto poc'anzi [51]- più in generale, il trattamento dei dati personali e la loro libera circolazione. Si tenderà pertanto a fare riferimento ai due strumenti in modo congiunto, tenendo in considerazione le rispettive differenze.

Occorre precisare che una parte delle tecniche di riconoscimento biometrico può essere impiegata nel contesto di spazi pubblici o per la prevenzione o il perseguimento di reati, nel cui ambito è necessario prescindere dal consenso dei soggetti interessati. Infatti, in ragione del bilanciamento tra diversi interessi in gioco poc'anzi richiamato, il consenso non potrebbe essere invocato legittimamente dai suoi titolari. Si tratta di un utilizzo consentito dal GDPR nel rispetto di una serie di requisiti, tra i quali si ricordano i motivi «di interesse pubblico rilevante» e l'esigenza che l'impiego sia «proporzionato alla finalità perseguita». Con riferimento al fondamento giuridico, esso dev'essere individuato sulla base «del diritto dell'UE o degli Stati membri». Più nel dettaglio, la direttiva 680/2016/UE autorizza il trattamento dei dati biometrici a fini di prevenzione e repressione dei reati, purché sia «strettamente necessario» rispetto alla presenza di specifiche giustificazioni per il trattamento di tali dati[52], in conformità al diritto dell'UE o degli Stati membri, e sia soggetto a garanzie adeguate per i diritti e le libertà dell'interessato[53]. In tal modo, la direttiva ripone negli Stati membri una "generica" responsabilità nell'introduzione di una disciplina attuativa idonea ai requisiti prefigurati. A dimostrazione di un'eccessiva vaghezza e genericità normativa che può generarsi a livello nazionale, il d.P.R. 15/2018 dispone che il trattamento dei dati biometrici sia consentito «quando è necessario per le esigenze di un'attività informativa, di sicurezza o di indagine di polizia giudiziaria o di tutela dell'ordine e della sicurezza ad integrazione di altri dati personali»[54]. D'altro canto, in accordo con l'orientamento maggioritario della giurisprudenza della Corte di giustizia[55], la direttiva rammenta la necessità di operare - più in generale - una distinzione tra le diverse categorie di destinatari interessati al trattamento, in rapporto alla specifica qualifica acquisita durante il procedimento penale[56], al fine di stabilire un bilanciamento più ponderato fra la tutela dei dati

[51] Cfr. *supra* il § 1.

[52] Così GRUPPO DI LAVORO - ARTICOLO 29, *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, WP 258, 29 novembre 2017, pp. 7 e ss.

[53] Cfr. il considerando n. 37 LED.

[54] Cfr. l'art. 11, c. 2 del d.P.R. n. 15/2018.

[55] Cfr. CGUE, C-203/15 e C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* e *Secretary of State for the Home Department v. Tom Watson e a*., 21.12.2016, par. 105.

[56] L'art. 6, della direttiva LED, rubricato "*Distinzione tra diverse categorie di interessati*", esorta gli Stati membri affinché «se del caso e nella misura del possibile, operino una chiara distinzione tra i dati personali delle diverse categorie di interessati, quali: a) le persone per le quali vi sono fondati motivi di ritenere che abbiamo commesso o stiano per commettere un reato; b) le persone condannate per un reato; c) le vittime di reato o le persone che alcuni fatti autorizzano a considerare potenziali vittime di reato; d) altre parti rispetto a un reato, quali le persone che potrebbero essere chiamate a testimoniare nel corso di indagini su reati o di

personali e le esigenze di repressione dei reati. In questo modo, infatti, sarebbe possibile assicurare un più elevato standard di tutela per il trattamento dei dati di soggetti del tutto estranei o non destinatari diretti dell'addebito[57].

Giova richiamare un ulteriore aspetto di particolare rilievo che concerne la tutela dell'anonimato nello spazio pubblico. Trattasi della disposizione avente ad oggetto la possibilità di prescindere dalla previsione legislativa di una disciplina posta a protezione del trattamento per fini di polizia, nel caso in cui questo avvenga perché i dati siano stati «resi manifestamenti pubblici dall'interessato»[58]. Per esempio, una videoripresa eseguita in una piazza aperta al pubblico a fini di prevenzione, potrebbe rientrare in tale ipotesi qualora emerga inequivocabilmente che l'interessato «abbia volontariamente rinunciato alla protezione speciale per i dati sensibili rendendoli disponibili al pubblico, autorità comprese»[59]. Si ritiene tuttavia che il semplice atto di transitare per quella piazza non dovrebbe di per sé legittimare le forze di polizia e di sicurezza a raccogliere le immagini dei passanti[60].

Gli strumenti normativi posti a tutela del trattamento dei dati biometrici in presenza di un "interesse pubblico" offrono l'occasione di specificare due ulteriori condizioni. In primo luogo risulta quantomai necessaria una disciplina normativa che specifichi ulteriormente il fondamento giuridico e i requisiti da rispettare per trattare questa particolare categoria di dati personali[61]. A tal proposito occorre che la legislazione interna sia determinata, prevedibile e adeguatamente accessibile, al fine di consentire alle persone di agire in conformità alla legge e delimitare nettamente la discrezionalità in capo alle autorità pubbliche[62]. In tal senso, la previsione dell'art. 52 par. 1 della CDFUE stabilisce espressamente che qualsiasi minima limitazione nell'esercizio dei diritti fondamentali - come per esempio la libertà personale intesa nella sua accezione più estesa - deve essere prevista dalla legge, implicando che la base giuridica che consente l'intrusione nell'esercizio di determinati diritti fondamentali, debba stabilire la portata esatta della limitazione dell'esercizio del diritto considerato[63]. Su questo punto sarà utile concentrare l'attenzione più avanti (cfr. il capitolo III, §§ 2 e ss.).

---

procedimenti penali conseguenti, le persone che possono fornire informazioni su reati o le persone in contatto o collegate alle persone di cui alle lettere a) e b)».

[57] Cfr. B. Galgani, *Habeas data e garanzie fondamentali*, cit., pp. 15 e 16.

[58] Cfr. l'art. 10, par. 1, lett. *c*), LED.

[59] GRUPPO DI LAVORO - ARTICOLO 29, *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, cit., p. 10.

[60] Stessa considerazione vale per le immagini che circolano su internet, come ad esempio nei *social network*. Su questo punto, v. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 158.

[61] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., pp. 158-159.

[62] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 160.

[63] Si tornerà su questo punto *infra* nel capitolo III quando si approfondirà l'analisi del *template* nello spettro delle garanzie processuali fondamentali. V. CGUE, parere 1/15 (Accordo PNR UE-Canada), 26.7.2017, 139; CGUE, C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems*, 16 luglio 2020, p. 175. A tal proposito, G. Mobilio, *Tecnologie di riconoscimento facciale*, cit. p. 161 sostiene che «*la normativa in questione, dunque, deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura* de qua *e impongano requisiti minimi in modo che le persone i cui dati sono*

Con riferimento al principio di proporzionalità[64], la valutazione dev'essere eseguita caso per caso, tenendo conto della limitazione dei diritti, dello scopo e del contesto di impiego. Per vero, l'applicazione del suddetto principio si collocherebbe in un contesto ermeneutico più ampio rispetto al precedente, dal momento che, in conformità a una specifica disposizione normativa, persegue un obiettivo più generale di tutela del contenuto essenziale del diritto. Ne consegue che, la proporzionalità vada valutata rispetto all'idoneità degli atti dei pubblici poteri posti in essere per realizzare gli scopi perseguiti dalla norma, senza che siano travalicati i limiti. Questo giudizio può effettuarsi tenendo necessariamente in considerazione anche altri elementi, tra i quali rientrano, per esempio, il settore interessato, la natura del diritto in gioco, la gravità dell'intrusione e la finalità di quest'ultima. È quanto viene specificato con riferimento alla possibilità di conservare dati biometrici a scopi di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali[65] o quando le autorità di sicurezza pubblica hanno la necessità di trattare tali dati per esigenze connesse all'interesse pubblico[66].

Tra i principi posti a tutela del trattamento dei dati biometrici a fini di prevenzione e repressione dei reati, assume poi un particolare rilievo il principio di "limitazione delle finalità". Sulla base di questo, i dati personali devono essere «raccolti per finalità determinate, esplicite e legittime» e «trattati in modo non incompatibile» con le stesse[67]. La *ratio* della disposizione è quella di rafforzare la libertà di autodeterminazione sui propri dati, esercitando su di essi, quantomeno indirettamente, una forma di controllo, prevenendo la violazione di diritti fondamentali mediante l'utilizzo non dichiarato dei dati o la loro violazione mediante un accesso illegittimo, e in questo modo promuovendo la fiducia nei destinatari del trattamento. Il legislatore europeo specifica che un possibile riutilizzo consentito dei dati raccolti (cd. "trattamento secondario") possa avvenire «a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici»[68]. In particolare, la direttiva, nel consentire l'accesso e il riutilizzo dei dati da parte delle forze di polizia, stabilisce che questo possa eseguirsi all'interno degli scopi rientranti nella più generica finalità della prevenzione e della salvaguardia

stati conservati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti».

[64] Cfr. il considerando n. 93 che richiama l'art. 5 TUE. Sul principio di "proporzionalità" cfr. *ex multis*, F. Nicolicchia, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Wolters Kluwer, 2020, pp. 107 e ss., M. Caianiello, *Conclusive remarks. Antifraud investigations and respect for fundamental rights faced with the challenge of e-evidence and digital devices*, in AA.VV., *Digital Forensic Evidence. Towards Common European Standards in Antifraud Administrative and Criminal Investigations*, (a cura di) M. Caianiello, A. Camon, Wolters Kluwer, 2021, p. 243 e S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigative*, Giappichelli, Torino, 2018, pp. 262 e ss.

[65] Cfr. CGUE, C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 38.

[66] Cfr. CGUE, C-362/14, *Maximillian Schrems*, cit., p. 87.

[67] Cfr. l'art. 4, par. 1, lett. *b*), LED.

[68] Cfr. l'art. 3, par. 4, LED.

contro minacce alla sicurezza pubblica. È chiaro che questo non può tradursi in una legittimazione a priori di riutilizzo dei dati per indagare su reati diversi da quelli per i quali sono stati raccolti. In questo senso, la disciplina nazionale reca un ambiguo articolo 13, c. 3 (d.P.R. n. 15/2018), che consente la comunicazione dei dati personali a pubbliche amministrazioni o enti pubblici e a privati quando risponde all'interesse della persona cui i dati si riferiscono e, comunque, nei singoli casi in cui è necessaria per evitare un pericolo grave e imminente per la sicurezza pubblica, o per la salvaguardia della vita e dell'incolumità fisica di un terzo. Sotto questo punto di vista, la Corte di giustizia ha stabilito in diverse pronunce come, al fine di procedere ad un legittimo riutilizzo dei dati raccolti, debbano essere necessariamente indicate le «condizioni sostanziali e procedurali», che devono determinare «criteri oggettivi» rigorosamente ristretti e idonei a giustificarne la nuova utilizzazione rispetto alla finalità perseguita[69]. Nel noto caso *S. & Marper*, anche la Corte europea dei diritti dell'Uomo ha affermato che, nel contesto di utilizzo di dati biometrici, occorre fare riferimento a regole chiare e dettagliate volte a disciplinare la portata e le modalità di applicazione delle misure nonché le garanzie minime riguardanti, fra l'altro, la durata, la conservazione, l'utilizzo, l'accesso ai terzi e le procedure di distruzione degli stessi, al fine di prevenire il rischio di abusi e riutilizzi arbitrari[70]. Il rispetto di tali condizioni, tuttavia, può sembrare piuttosto complesso per l'impiego di alcuni dati biometrici più facili da captare[71] e potenzialmente di più agevole cessione e circolazione. Per esempio, le tecnologie di riconoscimento facciale, come si avrà modo di approfondire meglio *infra*[72], consentono di rielaborare e trattare i dati con modalità e finalità che il titolare del trattamento difficilmente può immaginare al momento della raccolta. L'impiego di alcune tecniche di intelligenza artificiale (cfr. il capitolo II, § 2), poi, applicate nel contesto del trattamento di dati biometrici come l'immagine di un volto, può sfociare in alcune pratiche abusive denominate "*fishing expeditions*", ossia i cd. "rastrellamenti" di immagini, aventi la finalità generica di raccogliere informazioni sulla popolazione per scopi principalmente preventivi, ma il cui utilizzo potrebbe prestarsi anche per finalità repressive[73]. Pertanto, il principio di limitazione della finalità va applicato non solo a tutti gli stadi del

[69] Cfr. *ex multis* CGUE, C-362/14, *Maximillian Schrems*, cit., p. 93; CGUE, parere 1/15 (Accordo PNR UE-Canada), cit., par. 191.

[70] Cfr. C. Edu, *S. & Marper c. Regno Unito*, 4.12.2008, par. 99.

[71] Cfr. S. Rodotà, *Tecnologie e diritti*, Il Mulino, Bologna, 1995, p. 47, ha sottolineato come «le informazioni fornite dagli interessati per ottenere determinati servizi sono tali, per quantità e qualità, da determinare la possibilità di una serie di impieghi secondari, particolarmente remunerativi per i gestori dei sistemi interattivi».

[72] Cfr. *infra* il capitolo IV.

[73] Cfr. N. Strossen, *Post-9/11 Government Surveillance, Suppression and Secrecy*, in AA.VV., *Privacy, Security and Accountability. Ethics, Law and Policy*, (a cura di) A.D. Moore, Rowman & Littlefield, New York, 2016, pp. 226 e ss. Per un'analisi sulla distinzione fra le finalità di "*prevention*" e "*repression*", v. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, 2020, pp. 38 e ss.

procedimento penale, ma anche in una fase ancora precedente, garantendo così un collegamento costante tra la persona titolare dei dati e lo scopo del loro utilizzo[74].

Ulteriore principio fondamentale posto a presidio dei dati biometrici trattati a fini di prevenzione e repressione dei reati, è quello della minimizzazione dei dati. La *ratio* di base è costituita dalla limitazione della raccolta ai dati personali necessari per il raggiungimento della finalità consentita dalla legge, cancellando quelli non essenziali o non conformi allo scopo preposto. In tal senso, la direttiva fa riferimento alla necessità che i dati biometrici siano "adeguati" e "pertinenti" rispetto alle finalità per le quali sono trattati. In particolare, si precisa che i dati non devono eccedere rispetto alla finalità da perseguire, lasciando l'idea di un vincolo poco stringente in relazione all'obiettivo di pubblico interesse ad essa sotteso[75]. Il principio in esame assume una certa rilevanza al momento della conversione del campione biometrico in un'immagine digitale o in un modello elettronico: le caratteristiche estratte non devono essere eccessive ai fini della comparazione fra *template* e/o rappresentazioni digitali del tratto (cfr. *infra* il § 2.2) e devono riportare unicamente le informazioni richieste ai fini dell'utilizzo specificato[76]. Da una parte, i dati biometrici digitalizzati devono presentare una dimensione idonea per la tipologia di dati contenuti, utile alle finalità di trattamento, evitando la sovrapposizione di informazioni pleonastiche. Dall'altra, essi dovrebbero presentare una quantità di caratteristiche tali da consentire di risalire ai dati biometrici raccolti e a partire dai quali sono stati ricavati (cfr. *infra* il § 2.2).

Il principio di minimizzazione dei dati costituisce un criterio valido anche per la realizzazione delle cd. *watchlist* utili ai fini del riconoscimento facciale[77]. Si tratta di gallerie di immagini che sono utilizzate per confrontare i volti delle persone da riconoscere[78]. Tuttavia, come è stato osservato in dottrina, il concetto di minimizzazione dei dati mal si concilierebbe con l'applicazione di tecniche di *machine learning* che, come vedremo[79], richiedono una rilevante quantità di dati da processare[80]. Strettamente connesso a questo è il principio della "limitazione della conservazione", secondo cui i dati personali devono essere registrati e conservati in una modalità che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per cui sono stati trattati[81]. In altre parole, la conservazione dei dati biometrici deve rispettare criteri oggettivi, tenendo

[74] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit. p. 172.
[75] Cfr. l'art. 4, par. 1, lett. *c*), LED. In linea con questo l'art. 23, c. 2, del d.P.R. n. 15/2018, sebbene – si ricorda – le finalità di polizia ivi indicate siano espresse in termini parzialmente differenti dal d.lgs. n. 51/2018.
[76] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit. p. 174.
[77] Cfr. il capitolo IV, § 1.3.
[78] Per un approfondimento v. *infra* il capitolo IV.
[79] Cfr. *infra* il capitolo II, § 2.
[80] Cfr. M. Ebers, *Regulating AI and Robotics: Ethical and Legal Challenges*, in AA.VV., *Algorithms and Law*, (a cura di) M. Ebers, S. Navas Navarro, Cambridge University Press, Cambridge, 2020, p. 64.
[81] Cfr. l'art. 5, par. 1, lett. *e*) del GDPR, e dall'art. 4, par. 1, lett. *e*), LED.

sempre in considerazione il rapporto tra i dati da conservare e l'obiettivo perseguito. Per vero, la Corte europea dei diritti dell'Uomo ha avuto modo di aggiungere che «*the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences* (…) *fails to strike a fair balance between the competing public and private interests*» e, pertanto, «*the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society*»[82]. Ne consegue che, nel momento in cui sia venuta meno la motivazione che ha giustificato la raccolta dei dati, e in assenza di un ulteriore fondamento giuridico, sarà necessario procedere alla cancellazione dei dati stessi. Per specifici sistemi di riconoscimento biometrico, peraltro, l'obbligo di cancellazione si riferisce sia ai dati digitali sia ai tratti biometrici "grezzi" (cfr. *infra* i §§ 2 e ss.)[83]. In ogni caso, è necessario assicurare la cancellazione automatica dei dati nel caso in cui vi sia una mancata corrispondenza dei tratti biometrici considerati, mentre, in caso di corretta coincidenza, l'eliminazione dovrebbe avvenire in un tempo strettamente necessario agli scopi per i quali sussiste un legittimo fondamento. La conservazione dei dati risulta strettamente connessa ai principi di "integrità e riservatezza". In forza di questi, i dati devono essere trattati in modo da garantire un'adeguata sicurezza contro utilizzi illeciti o la perdita, la distruzione e i danni accidentali, predisponendo anche misure tecniche e organizzative adeguate[84]. Queste ultime sono poste a presidio dell'ulteriore principio di "sicurezza del trattamento", da valutare rispetto alla natura, all'oggetto, al contesto e alle finalità di utilizzo dei dati, come anche al rischio per i diritti fondamentali[85]. A titolo meramente esemplificativo, sia il GDPR sia la direttiva elencano una serie di obiettivi, tra i quali giova ricordare la "pseudonomizzazione" dei dati[86]. Tale operazione risulta finalizzata proprio alla prevenzione di una potenziale violazione o furto degli stessi.

Infine, con riferimento alle informazioni da fornire al soggetto interessato, mentre nel GDPR è stato valorizzato il diritto a ricevere informazioni da parte del titolare del trattamento prima che questo avvenga (cd. "autoderminazione informativa")[87], nella LED si distingue solamente fra "informazioni da mettere a disposizione" in termini generalizzati al pubblico e le ulteriori informazioni da fornire ad un determinato interessato "in casi specifici"[88]. In questo modo, viene strutturata un'informativa su più livelli, con un primo avvertimento nel luogo circostante l'acquisizione di un determinato tratto

[82] Cfr. C. Edu, *S. & Marper*, cit., 125.
[83] Per es. i sistemi di riconoscimento facciale, come si approfondirà meglio *infra* nel capitolo IV.
[84] Cfr. l'art. 5, par. 1, lett. *f*) del GDPR; art. 4, par. 1, lett. *f*), LED.
[85] Cfr. l'art. 32 del GDPR e l'art. 29, LED.
[86] Cfr. l'art. 32, par. 2 del GDPR e l'art. 29, par. 2, LED.
[87] Cfr. gli artt. 13 e 14 GDPR. Si tratta delle informazioni che il titolare del trattamento ha l'obbligo di fornire all'interessato, consentendogli di venire a conoscenza dell'esistenza di un trattamento in corso. Cfr. il capitolo IV, § 3.1.6.
[88] Cfr. l'art. 13, par. 1 e par. 2, LED.

biometrico, e un secondo con le ulteriori e più specifiche informazioni necessarie in formato più dettagliato. Un'altra differenza significativa della direttiva rispetto al GDPR riguarda le possibili limitazioni ai diritti e ai principi introdotti dalla relativa disciplina. Infatti, diversamente dal regolamento che garantisce comunque che le norme debbano presentare determinati contenuti minimi[89], la LED autorizza analoghe limitazioni dei diritti in rapporto alle diverse esigenze concrete dei procedimenti penali o agli interessi pubblici cui è preposta[90], non indicandone un contenuto minimo necessario. Ne deriva un quadro normativo interno agli Stati membri piuttosto frammentato. Per esempio, l'art. 10 c. 1 d.lgs. 51/2018 impone di mettere a disposizione del destinatario interessato alcune informazioni, tra le quali rilevano quelle che permettono di identificare il titolare del trattamento e le finalità dello stesso, oltre ad una serie di diritti tra cui il reclamo all'autorità di controllo *ex* art. 52 della direttiva, l'accesso ai dati *ex* art. 11 e la possibilità di rettifica, cancellazione e limitazione del trattamento secondo quanto stabilito dall'art. 12[91]. Tuttavia, come stabilito anche dalla Corte europea dei diritti dell'Uomo[92], il diritto di accedere a determinate informazioni personali e ai dati trattati deve essere bilanciato anche con gli interessi della sicurezza pubblica e della repressione dei reati. L'introduzione da parte della direttiva di questi diritti costituisce una significativa novità, sebbene si debba sempre tenere presente che essi possono essere limitati in determinate circostanze. In quest'ultimo caso, il destinatario interessato può comunque esercitare i suddetti diritti attraverso l'autorità di controllo (cd. "accesso indiretto")[93].

Infine, mentre il GDPR contempla espressamente il diritto a ottenere una limitazione del trattamento entro alcune ipotesi specifiche, come per esempio nel caso di dati personali parzialmente corretti o come alternativa alla cancellazione degli stessi[94], la direttiva non dedica un'apposita

[89] L'art. 23 par. 1 elenca le specifiche finalità per «la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica» (lett. *d*) oppure «altri importanti obiettivi di interesse pubblico generale» (lett. *e*) – che possono giustificare la limitazione ai diritti e le prerogative previste agli artt. da 12 a 22 e 34, nonché i principi all'art. 5. Al par. 2 indica i contenuti che le previsioni legislative limitative devono necessariamente assumere, ovvero: le finalità o le categorie di trattamento; le categorie di dati personali; la portata delle limitazioni introdotte; le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti; l'indicazione precisa del titolare del trattamento o delle categorie di titolari; i periodi di conservazione e le garanzie applicabili; i rischi per i diritti e le libertà degli interessati; il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa».

[90] Cfr. gli artt. 18 e 13, par. 3, LED.

[91] Con riferimento alle "informazioni ulteriori", esse devono essere espressamente previste e disciplinate da una legge o un regolamento e possono consistere esemplificativamente nel titolo giuridico del trattamento, il regime di conservazione, i destinatari dei dati etc. A. Ricci, *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento*, cit., p. 583.

[92] Cfr. C. Edu, *Murray c. Regno Unito*, 26.4.2016, 93; *Segerstedt-Wiberg e altri c. Svezia*, 6.6.2006, 88.

[93] Cfr. l'art. 17 LED.

[94] Cfr. l'art. 18 GDPR.

disciplina a tale attività, sebbene nei considerando 47 e 48 se ne riesca a intravedere quantomeno una traccia[95].

1.2. Proprietà dei tratti biometrici

Una volta chiarito che cosa s'intenda con il termine "biometria" e introdotte alcune nozioni di base sui fondamenti normativi del trattamento dei dati biometrici a fini di prevenzione e repressione dei reati, si ritiene utile soffermarsi sulla trattazione delle principali qualità caratterizzanti tali tratti.

Innanzitutto, giova distinguere fra caratteristiche di tipo "fisico", "fisiologico", e "comportamentale"[96]. Tra le prime, a titolo esemplificativo, rientrano le impronte digitali, l'iride, la retina, il volto, la mano, la forma dell'orecchio, l'odore del corpo e i pori della pelle. I dati biometrici "fisiologici" possono essere generati osservando le diverse funzioni corporee. A differenza dei sistemi di riconoscimento basati su dati biometrici "fisici", quelli aventi ad oggetto informazioni "fisiologiche" catturano la biomeccanica e il funzionamento interno degli individui. Alcuni esempi appartenenti a questa categoria sono l'elettrocardiogramma (ECG), i modelli di respirazione e l'elettroencefalogramma (EEG). I dati biometrici fisiologici richiedono un'osservazione dei soggetti che non può essere istantanea, in quanto catturano la variazione delle caratteristiche corporee.
A differenza dei dati biometrici "fisici", e similmente a quelli "fisiologici", i dati biometrici "comportamentali" richiedono invece un'osservazione degli individui che introduce una variabile temporale nella valutazione. Tra le caratteristiche "comportamentali" possono essere ricondotte la scrittura, la battitura sulla tastiera, la cadenza dell'andatura e la voce[97].

[95] Cfr. il considerando n. 47: «(…) le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire i dati selezionati verso un altro sistema di trattamento, ad esempio a fini di archiviazione, o nel rendere i dati selezionati inaccessibili. Negli archivi automatizzati la limitazione del trattamento dovrebbe essere assicurata, in linea di massima, mediante dispositivi tecnici. Il sistema dovrebbe indicare che il trattamento dei dati personali è stato limitato in modo da renderne evidente la limitazione. Tali rettifiche o cancellazioni di dati personali o limitazioni del trattamento dovrebbero essere comunicate ai destinatari a cui tali dati sono stati comunicati e alle autorità competenti da cui i dati inesatti provengono. I titolari del trattamento dovrebbero inoltre astenersi dal diffondere ulteriormente tali dati». Cfr. anche il considerando n. 48: «nel caso in cui il titolare del trattamento neghi all'interessato il suo diritto di informazione, accesso, rettifica o cancellazione di dati personali o limitazione di trattamento, l'interessato dovrebbe avere il diritto di chiedere che l'autorità nazionale di controllo verifichi la liceità del trattamento. È opportuno che l'interessato sia informato di tale diritto. Qualora l'autorità di controllo intervenga per conto dell'interessato, essa dovrebbe quanto meno informarlo di aver eseguito tutti i riesami o le verifiche necessari. È inoltre opportuno che l'autorità di controllo informi l'interessato del diritto di proporre ricorso giurisdizionale».
[96] Tale tassonomia non è da ritenersi universale: infatti alcune tipologie di dati biometrici potrebbero essere classificate in modo differente. Per esempio, non è rara la catalogazione di dati biometrici fisici e fisiologici in un'unica categoria.
[97] Cfr. B. Lavanya, H. H. Inbarani, *A Survey of Biometric Techniques*, in *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, 7, 2015 ove afferma che «*dynamic signature verification, keystroke dynamics and speaker verifications are examples of behavioral characteristics. Physiological characteristics include hand or finger recognition, facial characteristics, and iris recognition*».

Al fine di poter classificare una caratteristica fisica, fisiologica o comportamentale come "biometrica", essa deve rispettare alcuni parametri oggettivi[98]. Le proprietà sono essenzialmente le seguenti:

- *universalità*: la caratteristica deve essere "comune" all'intera popolazione;

- *unicità* o *singolarità*: il carattere deve presentare peculiarità tali da poterlo riferire ad un unico individuo (cd. "riferibilità individualizzante" o "distintività")[99];

- *invariabilità*: il dato deve mantenersi costante nel tempo e indipendente rispetto a qualsiasi variabile;

- *ammissibilità* o *accettabilità*: la misurazione deve rispettare l'integrità fisica della persona, poter essere condotta senza metodi invasivi, mentre l'acquisizione deve potersi ritenere accettabile da un'ampia percentuale della popolazione;

- *acquisibilità* o *misurabilità*: i dati devono essere tali da poter essere acquisiti senza tempi di attesa troppo lunghi o altre complicazioni;

- *riservatezza*: la procedura non deve violare la privacy della persona (v. *infra* il capitolo III § 2.4);

- *riducibilità* o *collezionabilità*: la caratteristica biometrica deve essere misurabile quantitativamente e inseribile in un sistema stabile di rilevazione di facile consultazione[100];

- *grado di gradimento*: indica il livello di apprezzamento della metodologia biometrica applicata da parte dell'utente.

Alcune caratteristiche, seppur siano dotate di *universalità*, come il peso, le dimensioni o il colore degli occhi e dei capelli, non sono convenzionalmente fatte rientrare nella categoria dei dati biometrici,

---

[98] Cfr. S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, Giappichelli, Torino, 2013, p. 134, S. Smyth, *Biometrics, surveillance and the law. Societies of restrict access discipline and control*, Routledge, New York, 2019, p. 22, G. Iovane, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza,* Aracne editore, Roma, 2008, p. 172, B. Lavanya, H. H. Inbarani, *A Survey of Biometric Techniques*, cit., R. V. Ramen, V.Yampoolskiy, *Biometrics: a survey and classification*, in *Biometrics*, vol. 11, no. 1, 2008, A. Jain, R. Bolle, S. Pankanti, *Biometrics. Personal identification in Networked Society*, Springer Science, New York, 1999, pp. 4 e ss., A. Monteleone, *Rilevazioni biometriche : lo stato della "privacy" delle "networked people" tra il nuovo Codice ed i provvedimenti del Garante italiano*, in *Diritto&Diritti*, giugno 2004, p. 1, S. Bisi, *Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica*, in *Ciberspazio e diritto*, 2005, 1, pp. 3 e ss., G. Gerra, *Alcune tecniche di identificazione biometrica di pratica attuabilità*, in *Rivista giuridica sarda*, 2001, 1, pp. 303 e ss., M. Pulice, *Sistemi di rilevazione di dati biometrici e privacy*, in *Il lavoro nella giurisprudenza*, 2009, 10, pp. 994 e ss., T. Perfetti, *Biometria tra privacy e sicurezza*, in www.computerlaw.it (ultima visualizzazione 19.11.2020), A. North-Samardzic, *Biometric Technology and Ethics: Beyond Security Applications*, in *Journal of Business Ethics* (2020) 167, p. 435, R.D. Luis Garcia, C. Alberola Lopez, O. Aghzout, J. Ruiz Alzola, *Biometric identification systems*, in *Signal Processing* 83(12), pp. 2539-2557, 2003, D. Meuwly, N. Baker, *Biometrics in the aliens' identity chain. A literature study final report* (WODC PROJECT 2965), p. 30, reperibile all'indirizzo https://repository.wodc.nl/bitstream/handle/20.500.12832/2428/2965_volledige_tekst_tcm28-442367.pdf?sequence=3&isAllowed=y (visualizzato in data 4.10.2021).

[99] Simon Deignan, del Dipartimento per le minacce transnazionali del Segretariato OSCE, ha spiegato che «l'importanza dei dati biometrici risiede nel fatto che molte di tali caratteristiche sono uniche. In altre parole, la misurazione del viso, le linee tracciate dai vasi sanguigni e persino il modo di camminare sono tutti attributi che variano da un individuo all'altro». OSCE (Organization for Security and Co-operation in Europe), *La biometria al servizio della sicurezza dei cittadini*, 5.4.2019.

[100] In altre parole, il campione biometrico grezzo, per assumere rilevanza a scopi di verifica, identificazione o categorizzazione automatica, deve poter essere registrato e conservato all'interno di una banca dati.

in quanto non soddisfano alcuni dei suddetti criteri[101]. Infatti, alcuni tratti presenti in ciascun individuo non presentano un'alta *riferibilità individualizzante* (per esempio il peso), che permetta il riconoscimento espresso in percentuale del soggetto[102].

La tabella seguente riporta una classificazione esemplificativa sulla base di tre proprietà: *invariabilità, singolarità* e *accettabilità*[103].

Caratteristiche	**Tecnologia di acquisizione**	**Invariabilità**	**Singolarità**	**Accettabilità**
Geometria della mano	Ottica (IR)	Buona	1:1000	Molto buona
Geometria delle due dita	Ottica (IR)	Buona	1:1000	Molto buona
Retina	Ottica	Molto buona	1:10 milioni	Non buona
Iride dell'occhio	Ottica	Molto buona	1:6 milioni	Buona
Vene superficiali della mano	Ottica (IR)	Buona	Non nota	Molto buona
Firma	Dinamica (pressione)	Non buona	1:10000	Molto buona
Voce	Elettroacustica	Non buona	1:10000	Buona
Volto	Ottica o IR	Buona	Dipendente dal sistema	Buona
Impronte digitali	Ottica, capacitiva etc…	Molto buona	1:10 milioni	Buona

Tabella n. 1

Vi sono poi ulteriori distinzioni considerate nel contesto applicativo biometrico, a seconda dello strumento utilizzato per eseguire il riconoscimento[104]. Seguendo le considerazioni svolte con riferimento alla definizione di dati biometrici introdotta dal regolamento (UE) 2016/679 (cfr. *supra* il § 1), è possibile definire un "sistema biometrico" come qualsiasi strumento in grado di *riconoscere* le persone fisiche con un certo grado di probabilità, effettuando trattamenti tecnici specifici relativi alle caratteristiche fisiche, fisiologiche o comportamentali degli individui. Un "sistema biometrico" può

[101] Per esempio, la singolarità, la misurabilità o l'invariabilità. Cfr. G. Iovane, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza*, cit., p. 173.

[102] Tali dati rientrano nella categoria dei cd. "*soft biometric data*", oggetto di un ambito di ricerca relativamente recente. Alcuni ricercatori stanno cercando di colmare il divario tra le misure tecniche e la semantica umana in cui sono impiegate alcune etichette per l'individuazione e la descrizione di certi tratti (ad esempio, "alto", "basso", "magro", "bianco", "nero", "asiatico", "timido", ecc.). Una delle applicazioni più rilevanti potrebbe avvenire nell'ambito delle indagini di polizia in cui le descrizioni (come quelle fornite dai testimoni oculari) potrebbero essere di ausilio agli investigatori per l'identificazione degli individui.

[103] La tabella è tratta da G. Iovane, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza*, cit., p. 172.

[104] Cfr. J. Wayman, *Biometric Systems, Technology, Design and Performance Evaluation*, Springer, London, 2004.

comprendere un modulo di acquisizione dei dati (per esempio una telecamera o altri tipi di sensori), un software di mappatura biometrica e una banca dati per la registrazione e memorizzazione degli stessi. Come si approfondirà meglio *infra*, al capitolo II, è possibile applicare a tali sistemi di riconoscimento specifiche tecniche di intelligenza artificiale che permettono risultati più veloci ma non sempre completamente affidabili.

I sistemi di riconoscimento possono essere:

- *manifesti* o *occulti*: a seconda che l'utente sia o meno a conoscenza di essere sottoposto ad un sistema di riconoscimento biometrico (la maggior parte delle applicazioni sono manifeste)[105];

- *contestuali* o *differiti*: a seconda che il riconoscimento di persone fisiche avvenga contestualmente, mediante il confronto di dati biometrici estratti a distanza dalla persona con quelli contenuti in una banca-dati di riferimento, senza che l'utente ne sia a conoscenza, ovvero con un ritardo significativo rispetto alla cattura del dato da parte del sensore[106];

- *caratterizzati da utenti abituati all'utilizzo di tecnologie biometriche o meno*: a seconda che la popolazione degli utenti abbia o meno esperienza nell'uso dei sistemi biometrici;

- *presidiati o meno*: a seconda che il sistema sia o meno supervisionato o assistito da un operatore;

- *in condizioni ambientali standard* o *meno*: a seconda che il sistema si trovi o meno ad operare con valori di temperatura, umidità e soprattutto illuminazione che ricadono in un determinato intervallo di tolleranza;

- *pubblici* o *privati*: a seconda che il sistema sia gestito da autorità pubbliche (es. un controllo automatico di frontiera) oppure da privati (es. accesso alla propria abitazione);

- *aperti o chiusi*: a seconda che i dati biometrici acquisiti risiedano unicamente nel luogo logico o geografico dell'applicazione o che possano essere esportati per altre applicazioni.

Ulteriori classificazioni prevedono anche: (a) la distinzione tra applicazioni *cooperative* o *non cooperative*, a seconda che siano o non siano necessari il consenso e la collaborazione dello stesso soggetto per realizzare la procedura di autenticazione/identificazione/categorizzazione; (b) la distinzione tra *verifica*/*identificazione biometrica positiva*, in cui il soggetto fornisce la prova biometrica che effettivamente appartiene a un dato insieme, e *negativa*, in cui il soggetto afferma in base a proprie credenziali biometriche di non appartenere allo stesso[107].

---

[105] Alcuni strumenti possono essere utilizzati con modalità occulte per determinate indagini di polizia oppure per il mantenimento della sicurezza e dell'ordine pubblico. Cfr. S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, Giappichelli, Torino, 2013, pp. 135-136 e COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, 26.11.2010.

[106] Cfr. il capitolo IV, § 1.3.

[107] Cfr. S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo,* cit., p. 136 e COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, 26.11.2010.

2. Il "ciclo della prova biometrica": dal corpo "fisico" al corpo "elettronico"

Chiarite le caratteristiche fondamentali dei tratti biometrici, si ritiene doveroso far cenno a quello che potrebbe essere definito come "ciclo della prova biometrica": si affronteranno in particolare i principali passaggi che dall'acquisizione del campione biometrico grezzo portano alla costituzione dell'immagine digitalizzata o del "corpo elettronico" (ossia la cd. rappresentazione digitalizzata del tratto e il relativo *template*)[108].

L'evoluzione della scienza biometrica e, in generale, delle tecniche di trattamento dei dati biologici ha avuto un'incidenza di rilievo sul corpo del vivente. Quest'ultimo è in grado di fornire indicazioni particolarmente utili per l'accertamento del reato[109], anche a prescindere dall'atteggiamento partecipativo del suo titolare. Il corpo è divenuto col tempo, dunque, un oggetto giuridico "nuovo"[110] e uno strumento in continua trasformazione[111].

Anche a seguito del rilevante progresso scientifico, il corpo umano ha perso il suo carattere "unitario" per scomporsi in prodotti, organi, tessuti e cellule che possono essere separati dal corpo fisico d'origine, e circolare, mantenendo una propria natura autonoma. Tale destrutturazione si è acuita, soprattutto, quando al dato fisico si è iniziato a contrapporre la sua immagine digitalizzata. Le componenti fisiche del corpo e, più in particolare, i dati biometrici *tout court*, assumono rilevanza allorquando si dimostrano uno strumento indispensabile per la definizione e il riconoscimento dell'identità del soggetto. In tal senso, l'apporto scientifico consente di analizzare elementi e dati provenienti dal corpo, impensabili fino a pochi anni or sono. Dalla minima inflessione della voce ai movimenti dei muscoli facciali, l'evoluzione tecnologica consente di analizzare diversi dettagli che possono essere assunti come prova di una partecipazione ai fatti per cui si procede[112].

---

[108] L'analisi giuridica della rapresentazione digitale di un dato biometrico e del modello elettronico sarà oggetto del successivo capitolo II.

[109] Come sostiene C. Bonzano, *Gli accertamenti medici coattivi. Legalità e proporzionalità nel regime della prova*, Wolters Kluwer, Milano, 2017, p. 2 «la persona rappresenta da sempre – e dunque a prescindere dal sistema processuale di riferimento – la più allettante tra le prove e, al contempo, la più sensibile tra di esse: esprime un innato ed insopprimibile "interesse accertativo", che viene in rilievo sotto vari profili, al mutare dei quali cambiano i diritti individuali di riferimento e, per l'effetto, i modelli di tutela che debbono ritenersi operanti».

[110] Così S. Rodotà, *Ipotesi sul corpo "giuridificato"*, in *Tecnologie e diritti*, Bologna, 1995, p. 204 e M. Gialuz, *L'accesso al corpo tramite strumenti diagnostici*, in AA.VV., *Le indagini atipiche*, (a cura di) A. Scalfati, Giappichelli, Torino, 2014, p. 289.

[111] Cfr. T. Alesci, *Il corpo umano come fonte di prova*, Wolters Kluwer, Milano, 2017, pp. 57 e ss. e S. Rodotà, *Trasformazioni del corpo*, in *Pol. dir*., 2006, pp. 3 e ss.

[112] «Si torna così a dare rilievo, in modo nuovo, al corpo, che diventa fonte di altre informazioni, oggetto di un continuo "*data mining*", una miniera a cielo aperto dalla quale attingere dati ininterrottamente. Il corpo in sé sta diventando una password. La fisicità prende il posto delle astratte parole chiave, sostituite da impronte digitali, geometria della mano o delle dita o dell'orecchio, iride, retina, tratti del volto, odori, voce, firma, uso di una tastiera, andatura, Dna». T. Alesci, *Il corpo umano come fonte di prova*, cit., pp. 57 e ss. e S. Rodotà, *Trasformazioni del corpo*, in *Pol. dir*., 2006, pp. 58-59.

I rilievi e gli accertamenti che incidono sul corpo da cui si ricavano dati biometrici grezzi sono eterogenei, classificabili anche attraverso il differente grado di coercibilità in essi implicato[113]. Alcuni riguardano l'aspetto esteriore del soggetto, eseguibili anche coattivamente[114]; altri incidono sulla "sfera intima", tutte le volte in cui le indagini hanno ad oggetto parti del corpo non facilmente visibili; altri ancora sono effettuati con metodi invasivi. A quest'ultima categoria sono ascrivibili le ispezioni, le perquisizioni e gli accertamenti urgenti, che possono comportare anche il prelievo di materiale biologico.

A fronte di tale quadro complessivo, la prospettiva della presente ricerca impone di svolgere ampie riflessioni per riconoscere al corpo - anche smaterializzato in un modello elettronico - ed al suo titolare «diritti specifici di protezione dalle pretese conoscitive dell'autorità»[115] (cfr. *infra* il capitolo III, §§ 2 e ss.). A tal proposito, siffatta analisi non può prescindere dall'esame delle diverse tipologie di operazioni che possono essere compiute per il reperimento di dati biometrici, ottenibili sotto forma sia di campioni grezzi che direttamente da immagini digitalizzate[116].

In generale, tra le attività di reperimento di dati biometrici grezzi, rientrano certamente i rilievi e gli accertamenti eseguibili per identificare l'indagato, *ex* art. 349, comma 2 c.p.p., gli atti compiuti di propria iniziativa dalla polizia giudiziaria o su delega del pubblico ministero e volti all'assicurazione delle fonti di prova, *ex* art. 348 c.p.p., con eventualmente l'ausilio di persone idonee, ed infine, gli accertamenti ed i rilievi sulle persone, diversi dalle ispezioni personali, che possono essere eseguiti dagli ufficiali di polizia giudiziaria in situazioni di urgenza[117]. Con riferimento ai primi, come noto, l'identificazione biologica viene compiuta in base a due gruppi di dati identificativi: somatici[118] e biometrici[119]. La *ratio* di tale attività è quella di identificare la persona nei cui confronti vengono svolte le indagini. In tal senso, l'art. 347 comma 2 c.p.p. attribuisce alla polizia giudiziaria il compito di

[113] Cfr. T. Alesci, *Il corpo umano come fonte di prova*, cit., p. 61.

[114] Per una panoramica sugli accertamenti medici coattivi si v. *ex multis* C. Bonzano, *Gli accertamenti medici coattivi. Legalità e proporzionalità nel regime della prova*, Cedam, Milano, 2017.

[115] Cfr. T. Alesci, *Il corpo umano come fonte di prova*, cit., p. 61.

[116] Mentre in questa prima parte della ricerca si approfondirà lo studio del dato biometrico, sia come campione grezzo sia come sua rappresentazione digitalizzata e *template*, nel capitolo III si affronterà il tema approfondendo gli istituti processual-penalistici coinvolti nonché le richiamate garanzie fondamentali.

[117] T. Alesci, *Il corpo umano come fonte di prova*, cit., p. 71. Per un'analisi in termini giuridico-processuali dell'attività investigativa che ordinariamente viene compiuta sulla scena del crimine dalla polizia giudiziaria, si v. A. Chelo, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, Cedam, Milano, 2014

[118] Tale categoria comprende i dati che riguardano il cd. "fenotipo", ossia come appare la persona al mondo esterno, come la fotografia sulla carta d'identità ovvero l'immagine estratta da un video eseguito dalla polizia giudiziaria.

[119] Fra le tecniche di riconoscimento biometrico figura altresì l'analisi del Dna che è stata ammessa tra di esse (ISO/IEC JTC1 SC 37) anche se per il momento non permette un utilizzo in modalità autenticativa in tempo reale. Quest'ultimo criterio, comunque, non è contemplato nelle diverse definizioni di tecnologie biometriche e quindi non impedisce di annoverare l'analisi del Dna tra di esse. COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, 26.11.2010, disponibile su http://bioetica.governo.it/media/1846/p95_2010_identificazione-corpo-umano-biometria_it.pdf (ultimo accesso il 10.1.2021).

comunicare «le generalità, il domicilio e quanto altro valga alla identificazione della persona nei cui confronti vengono svolte le indagini, della persona offesa e di coloro che siano in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti». L'articolo 349 c.p.p. segue una linea progressiva, dall'invito rivolto dalla polizia giudiziaria all'interessato di riferire le proprie generalità ed ogni altra notizia che possa essere utile ai fini identificativi, alla possibilità di eseguire – ove occorra[120] – rilievi dattiloscopici, fotografici e antropometrici[121] nonché altri accertamenti (comma 2)[122]. Con lo scopo di tipizzare le modalità di accertamento a fini identificativi, nel 2005, il legislatore ha introdotto nel corpo dell'art. 349 c.p.p., il comma 2 *bis*[123]. In particolare la disposizione attribuisce agli ufficiali e agli agenti di polizia giudiziaria, previa autorizzazione del pubblico ministero, la possibilità di procedere al prelievo coattivo di capelli e saliva, qualora lo stesso sia utile per l'identificazione dell'indagato[124].

Dalla poc'anzi descritta forma di identificazione, è necessario distinguere l'identificazione compiuta dalla polizia per finalità di sicurezza, svolta nel corso di operazioni preventive, a tutela della collettività, che gode di un'autonoma disciplina. *Ex* art. 11 d.l. 21.3.1978, n. 5, convertito con modificazioni dalla l. 18.5.1978, n. 191, l'identificazione va compiuta dagli ufficiali e agenti di polizia nei confronti di chi rifiuta di dichiarare le proprie generalità oppure rende dichiarazioni o esibisce documenti in relazione ai quali ricorrono sufficienti indizi per ritenere la falsità. Ai sensi dell'art. 4 TULPS[125], nei confronti di determinate persone pericolose o sospette, oppure cittadini stranieri non appartenenti all'Unione Europea che non sono in grado o si rifiutano di provare la propria identità, l'autorità di pubblica sicurezza è obbligata, per gli stranieri – ha facoltà, per gli altri – ad eseguire rilievi segnaletici, descrittivi, fotografici, dattiloscopici e antropometrici, diversi dalle ispezioni

[120] L'inciso consente il compimento dei suddetti accertamenti solo in via sussidiaria, allorché non si sia riusciti ad ottenere l'identificazione mediante la modalità di cui al primo comma, ovvero quando la persona si sia rifiutata di fornire le proprie generalità o siano sorti dubbi in merito a queste.

[121] Tale tipologia di segnalamento consiste nella misurazione di determinate parti del corpo (a titolo esemplificativo, si ricorda la statura, la lunghezza del tronco, l'apertura delle braccia): tutti questi dati (non individuabili come "biometrici") vengono, poi, classificati in gruppi entro i quali si individua il soggetto da identificare.

[122] Si tratta di una locuzione di chiusura della norma che lascia aperto il catalogo delle nuove tecnologie che l'evoluzione scientifica può fornire. Il comma 2 dell'art. 349 c.p.p. è stato oggetto di una recente modifica da parte dell'art. 2 della l. n. 134/2021 (in Gazz. Uff., 4 ottobre 2021, n. 237) – "*Delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari*". Sono stati aggiunti i seguenti periodi: «i rilievi (…) sono sempre eseguiti quando si procede nei confronti di un apolide, di una persona della quale è ignota la cittadinanza, di un cittadino di uno Stato non appartenente all'Unione europea ovvero di un cittadino di uno Stato membro dell'Unione europea privo del codice fiscale o che è attualmente, o è stato in passato, titolare anche della cittadinanza di uno Stato non appartenente all'Unione europea. In tale caso, la polizia giudiziaria trasmette al pubblico ministero copia del cartellino fotodattiloscopico e comunica il codice univoco identificativo della persona nei cui confronti sono svolte le indagini».

[123] La disposizione è stata introdotta dall'art. 10, d.l. 144/2005, convertito in l. 155/2005, recante "*Misure urgenti per il contrasto del terrorismo internazionale*". Cfr. sul punto R. E. Kostoris, *Prelievi biologici coattivi*, in AA.VV., *Contrasto al terrorismo interno e internazionale*, (a cura di) R. E. Kostoris, R. Orlandi, Giappichelli, Torino, 2006, pp. 343 e ss.

[124] Il ricorso a tali metodologie si ritiene sussidiario rispetto agli altri rilievi che si dimostrino inidonei all'identificazione. Cfr. A. A. Dalia, *Il prelievo coattivo di materiale biologico per l'identificazione dell'indagato e per l'acquisizione di elementi probatori*, in A.A.VV., *Le nuove norme di contrasto al terrorismo*, (a cura di) A.A. Dalia, Giuffrè, Milano, 2006, p. 285.

[125] TESTO UNICO DELLE LEGGI DI PUBBLICA SICUREZZA – Regio decreto, 18.6.1931, n. 773.

personali. In particolare, l'art. 7 TULPS prescrive che l'autorità di pubblica sicurezza possa identificare persone sospette o pericolose che possono mettere a rischio l'ordine pubblico mediante l'effettuazione di rilievi segnaletici descrittivi, antropometrici, fotografici e dattiloscopici.

Come noto, poi, tra le diverse attività di assicurazione delle fonti di prova e conservazione delle tracce di reato, dei luoghi, cose o persone ad esso pertinenti, rientrano senza dubbio gli accertamenti e i rilievi urgenti che la polizia giudiziaria compie, in attesa dell'intervento del pubblico ministero, ovvero, prima che questi abbia assunto la direzione delle indagini, anche sulla persona, ad eccezione dell'ispezione personale *ex* art. 354 c.p.p. Pur consapevoli della difficoltà di individuare una netta distinzione fra le due categorie[126], il termine "rilievo" alluderebbe ad un'attività meramente ricognitiva, mentre l'"accertamento" richiama un'idea di studio e valutazione critica di alcuni elementi, necessariamente soggettiva e tecnico-scientifica[127]. La condizione di urgenza sottolinea la natura derogatoria dell'attribuzione alla polizia giudiziaria di un'attività, in via generale, conferita al pubblico ministero. Ne consegue l'impossibilità per la polizia giudiziaria di compiere accertamenti tecnici di natura irripetibile[128]. L'esclusione di questi ultimi dal novero delle attività esercitabili dalla polizia giudiziaria, nell'immediatezza del fatto e di propria iniziativa, non definisce sufficientemente l'ambito applicativo degli "accertamenti" di cui all'art. 354 c.p.p. Tuttavia, si ritiene che la polizia giudiziaria, potendo avvalersi, *ex* art. 348 comma 4 c.p.p., di persone idonee a compiere atti e operazioni che richiedono specifiche competenze tecniche, possa certamente compiere rilievi esteriori quali la raccolta di impronte digitali o palmari, di eventuali macchie di sangue, nonché prelievi di tracce da polvere da sparo ovvero di sostanze stupefacenti.

Con riferimento ai prelievi biologici, finalizzati all'acquisizione del Dna[129], si inserisce la modifica dell'art. 354 per effetto dell'art. 10 comma 4 *ter* d.l. 27.7.2005, n. 244, coordinato con la legge di

---

[126] Cfr. S. Lorusso, *L'esame della scena del crimine nella contesa processuale*, in *Dir. pen. proc*., 2011, p. 264 e A. Scalfati, *Gli accertamenti tecnici dell'accusa*, in *Indice pen*., 1992, p. 130.

[127] Non a caso, peraltro, la Corte Costituzionale ha di recente escluso dal novero delle attività investigative di carattere scientifico per le quali è prevista, a pena di nullità, la presenza del difensore e del consulente tecnico (art. 360 c.p.p.), i rilievi e i prelevamenti di reperti utili per la ricerca di tracce biologiche. In particolare, la Corte ha dichiarato non fondate le questioni di legittimità costituzionale dell'art. 360 del codice di procedura penale, «ove non prevede che le garanzie difensive previste da detta norma riguardano anche le attività di individuazione e prelievo di reperti utili per la ricerca del DNA», sollevate, in riferimento agli artt. 24 e 111 della Costituzione. Il solo fatto che un atto di indagine abbia ad oggetto rilievi o prelevamenti utili per la ricerca del Dna non ne modifica la natura e non ne giustifica, di per sé, la sottoposizione ad un regime complesso come quello previsto dall'art. 360 c.p.p. Cfr. Corte Cost., 15.11.2017, n. 239, in *Proc. pen. giust*., 2018, pp. 486 e ss. Cfr. anche T. Alesci, *Il corpo umano fonte di prova*, cit., p. 82.

[128] Cfr. A. Chelo, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, cit., pp. 40 e ss.

[129] Il prelievo è diretto a sottrarre dal corpo umano quel materiale (parte di tessuto o liquido organico) necessario per l'esecuzione delle ricerche o di analisi. Esso si delinea come «una "manovra" dalla struttura composita, che scaturisce dalla intersezione di quattro direttrici, riconducibili all'ambito di intervento, alle modalità, all'oggetto e alle finalità perseguite». Cfr. T. Alesci, *Il corpo umano come fonte di prova*, cit., p. 128. Secondo G. Gabrielli, *Il prelievo coattivo di campioni biologici nel sistema penale*, Giappichelli, Torino, 2012, p. 21, «si tratta di una operazione che, anzitutto, interviene sulla realtà corporale dell'individuo; che vi interviene senza il suo consenso, contemplando il ricordo alla coercizione fisica per vincere l'eventuale resistenza, che vi interviene sottraendo al soggetto passivo una quantità di sostanza biologica tendenzialmente modesta, destinata alla comparazione

conversione 31.7.2005, n. 155, che ha esteso l'operatività del prelievo ematico alla fase iniziale dei rilievi e degli accertamenti urgenti previsti dall'art. 354 comma 3, permettendo alla polizia giudiziaria di prelevare coattivamente il materiale biologico, sia all'indagato che a terzi (cfr. *infra*, il § 3.6)[130]. L'interpretazione letterale della norma ha prestato il fianco a critiche da parte della dottrina che ne ha sottolineato i limiti e ha evidenziato il sorgere di un «autonomo mezzo di accertamento concesso agli organi investigativi» con un «preoccupante margine di discrezionalità»[131]. Con l'introduzione della legge n. 85 del 2009[132], è stato soppresso il secondo periodo del comma 3, riducendo l'ambito operativo della polizia giudiziaria alla sola ipotesi di prestazione del consenso della persona interessata[133]. Le norme di riferimento, innestate nel tessuto codicistico per effetto della legge 30.6.2009, n. 85 con cui l'ordinamento italiano ha attuato il Trattato di Prüm[134], sono l'art. 224 *bis*, relativo ai "provvedimenti del giudice per le perizie che richiedono il compimento di atti idonei ad incidere sulla libertà personale" e l'art. 359 *bis*, circa "il prelievo coattivo di campioni biologici su persone viventi".

E' possibile ricorrere alle tipologia di prelevamento di cui agli artt. 224 *bis* e 359 *bis* c.p.p. sul presupposto di un'assoluta indispensabilità per la prova dei fatti. Inoltre, ai sensi dell'art. 224 *bis* comma 5, il legislatore ha stabilito alcune regole di condotta che impongono all'organo procedente di adottare le tecniche meno invasive e di «eseguire le operazioni peritali nel rispetto della dignità e del pudore di chi vi è sottoposto»[135]. Nella scelta delle tecniche per l'esecuzione dei prelievi, dunque, devono essere preferite quelle meno invasive nei confronti dell'integrità psico fisica, della dignità e del pudore[136].

---

genetica; che vi interviene infine con l'obiettivo di contribuire alle finalità, proprie del procedimento penale, di accertamento del fatto storico e delle relative responsabilità».

[130] Giova sottolineare che la norma, come modificata dalla novella del 2005, faceva riferimento al prelievo di "materiale biologico", eseguibile con le modalità previste dal comma 2 *bis* dell'art. 349 c.p.p. Quest'ultima norma ha ad oggetto solo il prelievo di capelli e saliva e non di sangue. Pertanto, rimaneva dubbia anche la possibilità che si potesse procedere più specificamente al prelievo ematico vero e proprio, pur rientrando senz'altro nella categoria di prelievo di "materiale biologico".

[131] Cfr. C. Fanuele, *Dati genetici e procedimento penale*, Cedam, Padova, 2009, p. 108.

[132] Recante l'adesione al Trattato di Prüm sulla cooperazione transfrontaliera, diretto a contrastare il terrorismo, la criminalità transnazionale e la migrazione straniera. Cfr. *infra* il § 3.6.2.

[133] Cfr. G. Lago, *Banche dati DNA: raccomandazioni internazionali. Studio comparato con la legge 85/2009*, in *Giust. Pen*., 2010, I, c. 141 e ss.

[134] Il trattato è stato sottoscritto con la finalità del rafforzamento della cooperazione internazionale con il precipuo compito di contrastare il terrorismo, la criminalità transfrontaliera e la migrazione illegale. La legge n. 85 del 2009 costituisce il primo e unico esempio di regolamentazione compiuta di un sistema di riconoscimento biometrico in Italia. La normativa è stata completata successivamente con l'introduzione di un regolamento attuativo, il d.P.R. n. 87 del 2016. Sul tema si veda C. Fanuele, *Dati genetici e procedimento penale*, Cedam, Padova, 2009 e AA.VV., *Banca dati del Dna e accertamento penale*, (a cura di) L. Marafioti, L. Luparia, Giuffrè, Milano, 2010.

[135] Cfr. A. Presutti, *L'acquisizione forzosa dei dati genetici tra adempimenti internazionali e impegni costituzionali*, in *Rivista italiana di diritto e procedura penale*, 2010, Vol. 53, fasc. 2, p. 552.

[136] Cfr. M. Chiavario, *Libertà*, III) *Libertà personale* (dir. proc. pen.), in *Enc. giur*. Treccani, Roma, 1993, 5 ss. e M. Chiavario, *Libertà personale e processo*, in *Processo e garanzie della persona*, II, terza ed., Giuffrè, Milano, 1984. V. anche G. Vassalli, *La*

Rimane fermo il fatto che la perizia costituisce la "sede naturale" del prelievo del dato biologico, poiché - come si avrà modo di approfondire più ampiamente *infra* - in quanto mezzo di prova, è garantita dalle forme del contraddittorio nella sua assunzione[137].

Peraltro, in forza del principio di solidarietà enunciato dall'art. 2 Cost.[138], i soggetti che possono subire prelievi di campioni biologici sono diversi: dall'indagato/imputato, alla persona offesa, - ai parenti dell'imputato[139] e ogni altro soggetto legato al procedimento. Al fine di determinare il profilo del Dna, il prelievo può avere ad oggetto i peli, i capelli e la mucosa del cavo orale[140]. Più controversa è l'espressione "accertamenti medici" che risulta eccessivamente generica, laddove permetta di eseguire operazioni aventi ad oggetto mere percezioni visive ovvero di introdurre strumenti all'interno del corpo di un individuo[141]. Le stesse modalità di prelievi possono essere determinanti già nella preliminare fase dell'investigazione: l'art. 359 *bis* c.p.p., infatti, richiama espressamente le operazioni di cui all'art. 224 *bis* c.p.p., omettendo, tuttavia, ogni riferimento alla controversa categoria degli accertamenti medici[142].

Le attività di reperimento di dati biometrici durante un procedimento penale si ascrivono ad una categoria assai ampia, dai confini non sempre precisamente tratteggiati e la cui acquisizione può essere il risultato di diverse e molteplici operazioni. Esso può essere reperito nella *scena criminis* attraverso determinati rilievi, ovvero, può essere prelevato coattivamente da un determinato soggetto, qualora le disposizioni codicistiche lo consentano. Il dato, a prescindere dalla sua provenienza originaria, risulta fondamentale per la ricostruzione del fatto e per l'accertamento della responsabilità: esso può essere un utile ausilio, sia in chiave investigativa sia in ambito probatorio, sotto forma di "campione biometrico grezzo" e sottoforma di immagine digitale, così da poter essere comparato con i dati digitalizzati o i *templates* presenti all'interno di una determinata banca-dati (cfr. *infra* il § 2.2).

2.1. Modello analitico di riferimento

Scopo primario della disciplina biometrica risulta quindi l'individuazione di dati sperimentali, dai quali è possibile trarre una vasta quantità di informazioni. Tra i diversi metodi analitici a cui si può

libertà personale nel sistema delle libertà costituzionali, in *Scritti in memoria di Piero Calamandrei*, Cedam, Padova, 1957, vol. V, pp. 353-408

[137] Cfr. T. Alesci, *Il corpo umano come fonte di prova*, cit., p. 134.

[138] Il quale impone anche a soggetti terzi di collaborare ed offrire il loro contributo all'accertamento dei fatti.

[139] In questi casi, una deriva assai pericolosa è rappresentata dalla pratica degli *screening* di massa, fenomeno già realizzatosi in Italia con riferimento al caso di Yara Gambirasio, la tredicenne scomparsa a Brembate di sopra ed uccisa circa 6 anni fa. Al fine di individuare l'autore del reato e per effettuare il confronto con il Dna ritrovato sugli slip della vittima, venne svolto un accertamento con diverse migliaia di prelievi genetici e comparazioni. T. Alesci, *Il corpo umano come fonte di prova*, cit., p. 134.

[140] Cfr. l'art. 224 *bis* co. 1 c.p.p.

[141] Cfr. *infra* il § 3.6.2 e il capitolo III, § 2.1.1.

[142] Cfr. C. Bonzano, *Gli accertamenti medici coattivi. Legalità e proporzionalità nel regime della prova*, Cedam, Padova, 2017.

ricorrere[143], il metodo biometrico consente un rilevante abbassamento della media ordinaria di errore, risolvendo, tra l'altro, anche il problema dell'incertezza che spesso pone il metodo induttivo, agevolando l'analisi dei risultati e delle modalità di sperimentazione dei dati[144]. L'analisi biometrica è caratterizzata da alcuni aspetti peculiari. *In primis* si riscontra l'elevata complessità e variabilità dei processi biologici rispetto ai quali risulta necessario prendere in considerazione una popolazione di riferimento[145]. Per tale ragione non è possibile formulare delle conclusioni in termini oggettivi ed assoluti[146]: queste sono espresse, infatti, in termini di valori medi, indici di variabilità e probabilità. In secondo luogo, la disciplina biometrica è basata su un numero di confronti indipendenti contenuti nei dati osservati. Tali misurazioni vengono eseguite "per gradi di libertà", quindi, una volta raggiunto un valore di soglia, questo viene scomposto per singole unità a partire dalle quali sono individuate, nello specifico, tutte le informazioni necessarie. Ne consegue che un sistema biometrico risulta essenziale nell'ambito di ricognizioni di persone basate su analisi vettoriali derivate, per esempio, da specifiche caratteristiche psicologiche e comportamentali del soggetto. Tali dati sono poi solitamente conservati in una banca-dati, oppure registrati in una *smart-card* dell'individuo.

2.2. Dall'*enrollment* al *template*: il procedimento di digitalizzazione biometrica

Il procedimento di riconoscimento biometrico comincia generalmente con la fase di *enrollment*[147], ossia con la registrazione dell'utente, mediante la rilevazione della caratteristica biometrica da parte del sensore e l'acquisizione della stessa sotto forma di dato biometrico, il cd. "dato biometrico grezzo" o "campione biometrico" (acquisito con una delle modalità indicate nel § 2), cui segue la sua

[143] Mentre il metodo "deduttivo" viene applicato al fine di dedurre determinate conseguenze a partire da alcune ipotesi, in modo che possano essere convalidate tramite specifiche osservazioni, il metodo "induttivo" si esegue effettuando delle generalizzazioni in cui il dato ottenuto viene considerato soggetto a mutazioni del tutto casuali.

[144] Cfr. K. Mather, *Elementi di Biometria*, Boringhieri, Torino, 1978, pp. 10-12 e G. Preite, *Il riconoscimento biometrico: Sicurezza vs. Privacy*, UNI service, Trento, 2008, pp. 1 e ss., ove l'Autore pone in luce i «vantaggi applicativi resi possibili anche dallo sviluppo delle tecnologie informatiche, e che si sostanzia nella notevole riduzione dei tempi di trattamento delle informazioni e nella possibilità di studiare un gran numero di caratteri qualitativi e quantitativi rilevati su più unità statistiche».

[145] Cfr. K. Mather, *Elementi di biometria*, cit., pp. 25 e ss.

[146] Non si possono formulare affermazioni di certezza ma solo di probabilità. Mather afferma infatti che «non possiamo definire con certezza la statura del prossimo uomo che incontreremo; ma quando sappiamo che una frazione m1 della popolazione presenta una statura y1, una frazione m2 presenta un valore y2 e così via, possiamo servirci delle frequenze relative come probabilità per dire che il prossimo uomo avrà una possibilità m1 di avere una statura y1, una probabilità m2 di avere una statura y2 e così via». K. Mather, *Elementi di Biometria*, cit., p. 25.

[147] Il processo automatizzato attraverso cui sono individuate e codificate le diverse caratteristiche dei dati biometrici grezzi ai fini della creazione del *template* è denominato "processo di estrazione delle caratteristiche". Si v. A. Monteleone, Rilevazioni biometriche: lo stato della "*privacy*" delle "*networked persons*" tra il nuovo Codice ed i provvedimenti del Garante italiano, in *Diritto&Diritti*, giugno 2004, p. 1 e A. K. Jain, K. Nandakumar, A. Ross, *50 years of Biometric Research: Accomplishments, Challenges, and Opportunities*, in *Pattern Recognition Letters*, Vol. 79, 2016, pp. 80-105.

conversione in un'immagine digitale (cd. "*biometric sample*")[148] e l'eventuale estrazione delle *features* fondamentali[149] per la costruzione del "*template*"[150] (cd. "*features extraction process*"), da intendersi come la descrizione dei caratteri fondamentali del tratto biometrico[151], con relativa conservazione in un dato *repository*. In tal senso, sia la rappresentazione digitale sia il *template* costituiscono una trasposizione digitale della caratteristica biometrica[152]. Per vero, come si approfondirà meglio *infra* al capitolo II § 1, un dato biometrico può essere la rappresentazione digitalizzata di un campione grezzo; può trovarsi sottoforma di *template*, frutto di procedimenti regolamentati di digitalizzazione; può essere ricavato da un video o da un'immagine memorizzata in un dispositivo tecnico specifico[153]; oppure può essere registrato in dispositivi IoT finalizzati ad un uso generico o commerciale, quindi estranei al procedimento penale, quali assistenti domestici o dispositivi elettronici di rilevamento delle proprie caratteristiche fisiologiche o comportamentali. Al fine di analizzare compiutamente il cd. "ciclo della prova biometrica" dalla fase di *enrollment* del dato sino alla sua trasformazione in modello elettronico, giova qui concentrarsi sul primo caso sopra richiamato, ossia il caso in cui sia in gioco un procedimento regolamentato di digitalizzazione lasciando l'approfondimento delle restanti due categorie al capitolo II, con il prospettato inquadramento giuridico.

---

[148] «*Analog or digital representation of biometric characteristics prior to biometric feature extraction*». Cfr. ISO/IEC 2382-37 (n. 24).

[149] «*In a second stage, the information contained in a sample is extracted, reduced, and transformed into labels or numbers via an algorithm*». C. Jasserand-Breeman, *Reprocessing of biometric data for law enforcement purposes: Individuals' safeguards caught at the Interface between GDPR and the "Police" directive?* Groningen, University of Groningen, p. 66, reperibile su https://research.rug.nl/en/publications/reprocessing-of-biometric-data-for-law-enforcement-purposes-indiv (visualizzato in data 22.9.2021).

[150] Giova sottolineare che, attualmente, per il funzionamento della maggioranza delle banche dati oggi in uso alle forze di polizia è sufficiente l'impiego dell'immagine digitalizzata del tratto biometrico, senza dover ricorrere al successivo passaggio di conversione in *template*, il quale comporta senz'altro costi più elevati dal punto di vista economico. Per vero, alcune tecniche di IA (cfr. il capitolo II, § 2) sono già di per sé in grado di estrarre automaticamente le *features* fondamentali dal tratto biometrico considerato e comparare i dati presenti all'interno del database. La fase che va dall'*enrollment* del dato biometrico alla conversione in immagine digitale e poi eventualmente in *template* costituisce il «(…) momento più delicato del sistema di registrazione delle informazioni biometriche per le implicazioni giuridiche che le modalità di trattamento dei dati sensibili possono riverberare sulla privacy». L. Cuomo, *Profili giuridici del trattamento biometrico dei dati*, in *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)*, fasc.1, 2014, p. 43. Sul punto si veda, Y. Chang, W. Zhang, T. Chen, *Biometric-based cryptographic key generation*, in *Proceedings of IEEE International Conference on Multimedia and Expo (ICME'04)*, Taipei, vol. 3, 2004, pp. 2203–2206, M. Senor, *Dal corpo fisico al corpo digitale e ritorno: la tutela della dignità digitale come garanzia di libertà*, in AA.VV., *Il corpo Digitale: natura, informazione, merce*, (a cura di) A. Marturano, Giappichelli, Torino, 2010, cit. p. 91 e A. Jain, S. Pankanti, *Biometrics Systems: Anatomy of Performance*, in *Ieice trans. fundamentals*, Vol. E00-A, NO, 1.1.2001, p. 4.

[151] A. Franco, D. Maio, *Introduzione ai sistemi biometrici*, in http://bias.csr.unibo.it/franco/SB/DispensePDF/1_Introduzione%20ai%20sistemi%20biometrici.pdf (visualizzato in data 12.5.2021). V. Provvedimento generale prescrittivo in tema di biometria – 12.11.2014, reperibile all'indirizzo https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992, definisce il *template* come «insieme di tratti biometrici memorizzati informaticamente e direttamente confrontabile con altri modelli biometrici». Il *template*, insieme all'immagine digitale del dato, sarà oggetto di un'analisi giuridica nel capitolo II.

[152] Un'immagine di un'impronta digitale, di un volto, dell'iride e così via.

[153] Sul punto cfr. G. Carlizzi, *La valutazione della prova scientifica*, Giuffrè, Milano, 2019, pp. 14-17 e M. H. Lim, A. B. J. Teoh, *Biometric Template Binarization*, in AA.VV., *Encyclopedia of Biometrics*, (a cura di) S.Z. Li, A.K. Jain, Springer, Boston, 2015.

Un sistema biometrico basico, poi, è costituito da quattro fondamentali elementi: un modello sensoriale che acquisisce il campione grezzo; la caratteristica estratta e "misurata" dallo *scanner*; la corrispondenza dei moduli nei quali le caratteristiche sono confrontate con i modelli di riferimento; infine, lo schema decisionale grazie al quale viene riconosciuta l'identità del soggetto. Il procedimento di trasformazione del dato biologico grezzo, prima in un'immagine elettronica, che costituisce la descrizione del tratto digitalizzato, e poi in *template*, implica una fase di campionamento, di quantizzazione elettronica e un processo di codifica[154]. Il dato campionato costituisce la grandezza biometrica ancora in forma analogica, mentre la quantizzazione consiste nella limitazione del numero di valori che una data grandezza può assumere. Più nel dettaglio, mentre la quantizzazione segmenta lo spazio di una determinata caratteristica biometrica in un numero di intervalli[155], la codifica assegna ad ognuno di questi ultimi un'"etichetta" binaria in modo tale che le caratteristiche possano essere mappate nel modello elettronico corrispondente[156].

---

[154] «*Biometric binarization is the process of converting real-valued biometric features into a binary string. For many modalities (e.g., face, fingerprint, and signature) where the extracted features are intrinsically real valued, biometric binarization is developed for transforming the features into an acceptable form of input to many template protection schemes such as fuzzy commitment, fuzzy extractor, secure sketch, and helper data systems. (…) Typical biometric binarization involves a quantization and an encoding process. Quantization segments a feature space into a number of intervals, and encoding tags each interval with a binary label so that features falling into an interval can be mapped to the corresponding binary label. When multiple feature spaces are involved, the individual binary outputs can be concatenated to form the final binary representation of a user*». M.H. Lim, A.B.J. Teoh, *Biometric Template Binarization*, in AA.VV., *Encyclopedia of Biometrics*, (a cura di) S.Z. Li, A.K. Jain, Springer, Boston, 2015.

[155] Vi sono diverse modalità di quantizzazione elettronica: univariabile, semi-multivariabile, multivariabile, statica e dinamica. La prima esegue la quantizzazione su ciascuna componente della caratteristica monodimensionale considerata, assumendo che le singole componenti siano indipendenti. La quantizzazione semi-multivariabile opera, invece, prendendo in considerazione diversi sottoinsiemi di più componenti di singole caratteristiche biometriche monodimensionali, presupponendo che a essere indipendenti siano i singoli sottoinsiemi. Il modello multivaribile esegue, invece, la quantizzazione direttamente su uno spazio della caratteristica tenendo conto di tutte le sue componenti. Infine, mentre la quantizzazione elettronica statica crea delle partizioni uguali su ciascuno spazio esistente nella caratteristica biometrica considerata, la quantizzazione elettronica dinamica migliora il tasso di falsi positivi e falsi negativi, creando un numero variabile di partizioni in ciascuno spazio del campione biometrico. Cfr. M. H. Lim, A.B.J. Teoh (2015) *Biometric Template Binarization*, cit.

[156] Giova ricordare che diversi studi dimostrano la possibilità di risalire a partire da un dato *template* non "crittografato" al campione biologico grezzo corrispondente. C. Jasserand, *Reprocessing of biometric data for law enforcement purposes: Individuals' safeguards caught at the Interface between GDPR and the "Police" directive?* cit., p. 68: « (…) *biometric templates are in fact partially reversible and could possibly regenerate information contained in biometric samples. In recent legal studies on the legal status of biometric data, authors have concluded that biometric templates are reversible, at least partially, and may not be considered as anonymous data anymore*». Su questo punto cfr. C. Kauba, S. Kirchgasser, V. Mirjalili, A. Uhl, A. Ross, *Inverse Biometrics: Generating Vascular Images from Binary Templates*, in *IEEE Transactions on Biometrics, Behavior, and Identity Science* (T-BIOM), 2021, J. Galbally, A. Ross, M. Gomez Barrero, J. Fierrez, J. Ortega-Garcia, *Iris Image Reconstruction from Binary Templates: An Efficient Probabilistic Approach Based on Genetic Algorithms*, in *Computer Vision and Image Understanding*, vol. 117, 10, pp. 1512 - 1525, 2013, A. Ross, J. Shah, A. K. Jain, *From Template to Image: Reconstructing Fingerprints From Minutiae Points*, in *IEEE Transactions on Pattern Analysis and Machine Intelligence, Special Issue on Biometrics*, vol. 29, no. 4, pp. 544-560, 2007, G. Mai, K. Cao, Pong C. Yuen, A. K. Jain, *On The Reconstruction Of Face Images From Deep Face Templates*, in the *IEEE Transactions on Pattern Analysis and Machine Intelligence*. Per un approfondimento sui modelli elettronici crittografati v. H. Kaur, P. Khanna, *Biometric template protection using cancelable biometrics and visual cryptography techniques*, in *Multimed Tools Appl* 75, pp. 16333–16361, 2016.

Il procedimento di digitalizzazione biometrica può essere misurato sulla base di tre criteri differenti: la prestazione, il livello di sicurezza e la tutela della riservatezza. La prima implica la capacità di classificare le rappresentazioni binarie di determinati dati biometrici ed è valutata positivamente quando sia in grado di estrarre le stesse perché dotate di un elevato carattere discretivo[157]. Il grado di sicurezza, invece, ha ad oggetto l'*output* del procedimento di conversione e può essere misurato usando il cd. "grado di entropia". Il livello di entropia del risultato può aumentare a seconda delle dimensioni delle caratteristiche prese in considerazione durante l'estrazione, ovvero modificando il numero delle segmentazioni presenti all'interno del campione biometrico di riferimento. In tal modo è anche possibile creare diverse rappresentazioni digitalizzate: più aumenta il grado di entropia di un determinato *output*, più diminuisce il livello di sicurezza e attendibilità del procedimento di conversione digitale[158].

Infine, durante il procedimento di digitalizzazione è necessario mantenere un elevato livello di protezione della riservatezza dell'utente, al fine di impedire la fuga di informazioni specifiche diverse da quelle oggetto di verifica per l'accesso ad un determinato sistema (cd. "*function creep*"). Pertanto, oltre ai dati biometrici specificamente considerati, risulta fondamentale proteggere ulteriori informazioni personali come l'origine etnica, il sesso e le condizioni sanitarie del soggetto[159]. Questi ultimi sono denominati dati cd. "ausiliari" e, al fine di evitare qualsiasi possibile violazione della privacy, non possono essere posti in relazione ai dati biometrici oggetto di estrazione, registrazione e conversione[160]. A ciò deve aggiungersi il pericolo connesso alle informazioni ricavabili indirettamente dal trattamento di questa particolare categoria di dati: le rilevazioni biometriche della struttura vascolare della mano possono rivelare malattie cromosomiche, così come la *signature recognition* può permettere di determinare la presenza di specifiche malattie neurologiche[161].

---

[157] «*Adequate preservation of significance of real-valued features (from the feature extractor) by the discretizer is important to guarantee good recognition accuracy. This requires the extracted binary representation to be at least as discriminative as the real-valued features. A better discretization includes a bit allocation process to ensure that only discriminative feature components are heavily weighted to obtain higher bit stability or accuracy in recognition performance*». M.H. Lim, A.B.J. Teoh, *Biometric Template Binarization*, cit.

[158] Pertanto, è consigliato l'utilizzo di specifiche tecniche di protezione e di criptazione dei dati: in particolare, si ricorre solitamente alle cd. "chiavi pubbliche" che, tuttavia, non sono considerate garanzia assoluta di sicurezza. Cfr. GRUPPO DI LAVORO, ARTICOLO 29, PROTEZIONE DEI DATI, *Parere 3/2005 riguardante l'attuazione del Regolamento (CE) N. 2252/2004 del Consiglio del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri*, in https://www.privacy.it/archivio/grupripareri200503.html (visualizzato in data 18.12.2020).

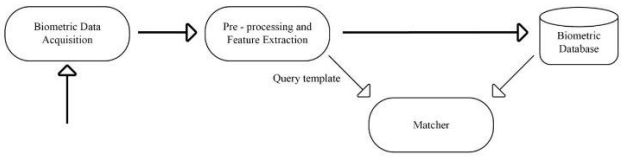
[159] Si tratta di vere e proprie operazioni di profilazione di soggetti. Per profilazione si intende «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica». Cfr. l'art. 4, par. 4 GDPR. L'elevato grado di rischio rappresentato dalla profilazione basata sull'utilizzo di dati biometrici viene evidenziata, in tal senso, dal legislatore europeo (cfr. il considerando 91).

[160] Cfr. M.H. Lim, A.B.J. Teoh, *Biometric Template Binarization*, cit.

[161] Cfr. COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, 26.11.2010.

2.3. (*Segue*) La fase del *matching*

Una volta conclusa la fase di *enrollment*, con contestuale conservazione del dato nel *repository*, si prosegue con il procedimento di comparazione o, direttamente delle immagini digitali, ovvero dei modelli elettronici, denominata "*matching*", al fine di determinare il loro grado di somiglianza e di correlazione[162].



Procedimento di *matching* in un sistema biometrico in modalità 1:N, 1:N+1 o 1:1

Nel procedimento di verifica o autenticazione, il confronto viene eseguito fra il dato biometrico digitalizzato archiviato mediante il procedimento di *enrollment* (*enrollment template*/*image*) e il *template*, o la rappresentazione digitale del tratto biometrico creato quando l'utente fornisce il proprio dato al dispositivo di rilevazione (*verification template/image*), il quale, a differenza del primo, viene in genere contestualmente cancellato.

In generale, al livello di somiglianza e correlazione viene assegnato un punteggio che, in un sistema biometrico standard, è valutato rispetto ad un predefinito valore di soglia[163]. Se il punteggio eccede quest'ultimo numero, si determina una combinazione (*match*) e, dunque, il soggetto viene riconosciuto, in caso contrario la corrispondenza risulterà mancata e non avrà luogo alcun *match* (*non-match*)[164]. Fermo restando che ciascuna immagine digitale o *template* risultano unici e irripetibili, le

[162] Cfr. G. Formici, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i legislatori e le Corti*, in *Saggi – DPCE online*, 2019/2, p. 1111, J. N. Pato, L. I. Millett, *Biometric Recognition: Challenges and Opportunities*, in *The National Academies Press* at http://www.nap.edu/catalog.php?record_id=12720, p. 2, A. Jain, R. Bolle, S. Pankanti, *Biometrics. Personal identification in Networked Society*, Springer Science, New York, 1999, p. 28.

[163] 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.

[164] Cfr. *infra* il § 2.4. «(...) in funzione del superamento di una soglia prestabilita, il sistema può validare una "Verifica di Identità" oppure, in modalità Identificazione, generare una lista di possibili candidati caratterizzati da un punteggio di "accoppiamento" (*matching*); il sistema attribuisce alla persona oggetto della transazione l'identità del candidato con il migliore punteggio di "accoppiamento"». COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, 26.11.2020. «E' poco probabile che due campioni della stessa caratteristica biometrica, acquisiti in diverse sessioni, coincidano perfettamente: 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».

due stringhe di dati, quella archiviata e quella ottenuta "in tempo reale", saranno sempre diverse. A tal proposito, nella maggior parte dei comuni sistemi biometrici, il dispositivo di cattura (*sensor*) è regolato da un algoritmo che consente in poco tempo di confrontare diversi modelli elettronici per verificarne il grado di correlazione, che in ogni caso non potrà essere totale, e determinare se esso ricada, in base al punteggio attribuito, al di sopra o al di sotto della soglia considerata accettabile.

Ne consegue che, posto che non è possibile in alcun caso raggiungere un grado di somiglianza pieno tra i dati confrontati, il risultato che il sistema biometrico può fornire ai fini del riconoscimento di un soggetto non può che essere approssimativo[165]. In altre parole, mentre una password offre risposte definite in termini di *matching* benché il metodo non sia più considerato sicuro[166], i sistemi biometrici non risultano ancora in grado di restituire un risultato altrettanto accurato, sebbene siano di più complessa violazione.

2.4. Le modalità di *verifica, identificazione* e *categorizzazione* biometrica

Le modalità attraverso cui un utente può essere riconosciuto da un punto di vista tecnico sono principalmente tre[167]. Ci si può, infatti, basare su qualcosa che l'utente conosce (una password o un codice *pin*), su qualcosa che l'utente possiede (un dispositivo di autenticazione, un *token* o una *smart card*) e, infine, su qualcosa che è proprio del soggetto, ossia, un tratto biometrico[168]. Si tratta di una distinzione particolarmente significativa che presuppone che l'"essere" sia in una relazione consequenziale con "l'accedere" e, quindi, l'essere coincida con il riconoscere. Solo sulla base di se stessi, del proprio corpo, è possibile, così, essere riconosciuti dal sistema[169]. L'aspetto più significativo

---

Sia consentito il rinvio a E. Sacchetto, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2/2019, p. 469.

[165] Non si può infatti parlare di una assoluta infallibilità dei sistemi di riconoscimento biometrici: si sono rilevati casi in cui la procedura identificativa ha presentato margini di errore anche a causa di mutamenti delle parti del corpo interessate, legate talvolta a determinate malattie (secchezza dell'epidermide, assottigliamento delle creste papillari, deterioramento dei polpastrelli, mutamento della struttura retinale dovuta a forme gravi di diabete, glaucoma, pressione alta). Per approfondimenti sul punto Cfr. AA.VV., *Biometric Systems. Technology, Design and Performance Evaluation*, (a cura di) J. Wayman, A. Jain, D. Maltoni, D. Maio, Springer, London, 2005.

[166] «*The traditional authentication method, such as PIN, is neither secure enough nor convenient for automatic identification system (…). (…) conventional password and Personal Identification Number (PIN) commonly used are insecure, requiring the user to change the password or PIN regularly*». C. T. Pang, Y. W. Yun, X. Jiang, *On-Card Matching*, cit.

[167] Cfr. A. Jain, R. Bolle, S. Pankanti, *Biometrics. Personal identification in Networked Society*, Springer Science, New York, 1999, pp. 3 e ss.

[168] La distinzione si ritrova in diversi autori, tra cui si ricorda E. Sanna, *Le garanzie di sicurezza e autenticità delle informazioni in rete*, in *Riv. giur. sarda*, 2001, fasc. 1, p. 311, S. Bisi*, Il furto d'identità: panoramica attuale e prospettive giuridiche*, in *Ciberspazio e diritto*, 2004, p. 316 e S. Bisi, *Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica*, in *Ciberspazio e diritto*, 2005, p. 9.

[169] Per un approfondimento sul punto cfr. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., pp. 60 e ss. e E. Mordini, *Il Volto e il Nome. Implicazioni Etiche, Sociali e Antropologiche delle Tecniche di Identificazione Biometriche*, *MEDIC*, 2006, 14, p. 39.

della disciplina, pertanto, deriva da un dato oggettivo: fra tutte le tecnologie di *automated identification and data capture*, la biometria si basa non su qualcosa che viene comunicato o fornito da un'autorità garante, ma su ciò che si è[170]. A tal proposito, una significativa distinzione riguarda la finalità che si propone la scienza biometrica, ossia categorizzare, determinare, ovvero verificare l'identità del soggetto[171]. Nell'ultima delle tipologie individuate si tende ad eseguire «il confronto di un campione biometrico presentato con il corrispondente dato biometrico registrato, relativo ad una singola persona»[172], al fine di accertare che l'individuo sia realmente chi dichiara di essere[173]. I sistemi biometrici di autenticazione/verifica accertano, quindi, la compatibilità fra due dati, effettuando un raffronto di tipo "*one to one*" (1:1) fra determinate caratteristiche, fisiche o comportamentali - già trasformate in *templates* o semplicemente convertite in immagini digitali - e un *set* di valori precedentemente fornito dallo stesso utente e registrato in un *database* o in un dispositivo mobile[174].

---

[170] «Si ricorre sempre più frequentemente a questi dati biometrici non solo per finalità d'identificazione o come chiave per l'accesso a diversi servizi, ma anche come elementi per classificazioni permanenti, per controlli ulteriori rispetto al momento dell'identificazione o dell'autenticazione/verifica, cioè della conferma di una identità». T. Alesci, *Il corpo umano come fonte di prova*, Wolters Kluwer, Milano, 2017, pp. 57 e ss. Cfr. anche S. Rodotà, *Trasformazioni del corpo*, in *Pol. dir*., 2006, p. 59, N.K. Ratha, J. H. Connell, R. M. Bolle, *Enhancing security and privacy in biometrics-based authentication systems*, in *IBM Systems Journal* 40, 3, pp. 614–634, 2001, Y. Lee, J. J. Filliben, R. J. Micheals, P. J. Phillips, *Sensitivity analysis for biometric systems: A methodology based on orthogonal experiment designs*, in *Computer Vision and Image Understanding* 117, 5, pp. 532–550, 2013, e E. Mordini, C. Ottolini, *Implicazioni etiche e sociali della biometria*, in *L'arco di Giano*, 2005, n. 45, p. 67.

[171] Cfr. G. Iovane, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza*, Aracne editore, Roma, 2008, pp. 171 e ss., A. Jain, R. Bolle, S. Pankanti, *Biometrics. Personal identification in Networked Society*, Springer Science, New York, 1999, pp. 2 e ss., W. S. Coats, A. Bagdasarian, T. J. Helou, T. Lam, *The practitioner's Guide to Biometrics*, *American Bar Association*, Chicago, 2007, pp. 5-6, J. L. Wayman, *Biometric Verification/Identification/Authentication/Recognition: The Terminology*, in AA.VV., *Encyclopedia of Biometrics*, cit., A. K. Jain, Arun Ross, S. Prabhakar, An Introduction to Biometric Recognition, in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, 2004, C. Giustozzi, *Giuristi e informatici divisi da una lingua comune: autenticazione?*, in http://www.interlex.it/forum10/relazioni/24giustozzi.htm (visualizzato in data 12.11.2020).

[172] Cfr. COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE 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*».

[173] Cfr. S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo,* cit., p. 135 e J.L. Wayman, *Fundamentals of biometric authentication technology*, in *Proceedings CardTech/Securtech*, Chicago, 1999.

[174] Cfr. S. Bisi, *Il furto d'identità: panoramica attuale e prospettive giuridiche*, cit., p. 314. «Rientra in questa categoria la verifica dell'identità di un soggetto in possesso di uno *smartphone* mediante l'uso del lettore di impronta digitale, inserito nel dispositivo elettronico. Un software dedicato stabilisce infatti la corrispondenza tra l'impronta raccolta al momento della verifica (quando cioè l'utilizzatore vuole accedere al proprio device) e quella memorizzata e conservata nel dispositivo stesso sin dalla sua configurazione. Ancora è il caso delle Carte d'Identità Elettroniche, munite di *chip*, all'interno del quale è contenuta una copia delle impronte digitali raccolte al momento della erogazione del documento; nel caso in cui si volesse verificare l'identità del possessore del documento, verrà effettuato un *match* tra il dato biometrico fornito al momento del controllo e quello immagazzinato nel *chip* del documento. Ben si comprende come il confronto sia uno-a-uno: il dato 'sorgente', da confrontare con quello di volta in volta fornito, è infatti solo uno». G. Formici, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, in Saggi – *DPCE online*, 2019/2, p. 1111. Oppure un altro esempio paradigmatico si trova disciplinato nella direttiva 2015/2366/UE del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, recepita in Italia dal d.lgs. 15 dicembre 2017, n. 218, che introduce il sistema di "autenticazione forte del cliente", il quale prevede per alcune tipologie di pagamento l'autenticazione basata sull'uso di due o più elementi (art. 97), uno dei quali può essere biometrico, come ad esempio il riconoscimento facciale. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., p. 120.

I dati biometrici sono elaborati matematicamente e registrati all'interno della memoria di una base di dati centralizzata, al fine di poter eseguire il cd. *match* con l'identità richiesta[175]. Il soggetto potrebbe possedere altresì una *smart card* ovvero un *chip* integrato in un documento d'identità, in cui sia archiviato e conservato un suo dato biometrico, tramite il quale, davanti al dispositivo di cattura, ben potrebbe essere effettuato un confronto tra il dato rilevato in tempo reale e quello registrato nel supporto[176].

L'"identificazione" consiste, invece, in un procedimento di attribuzione dell'identità che si realizza attraverso il raffronto dei dati biometrici di un soggetto ignoto con tutti quelli archiviati e registrati in un *database*[177], eseguendo così un confronto "*one to many*" (1:N, 1:N+1)[178]. Il sistema biometrico restituisce un risultato positivo o negativo, espresso tramite una determinata percentuale di compatibilità, a seconda che l'individuo appartenga o meno al gruppo di utenti noti al sistema[179]. Generalmente, a ogni *template* contenuto nell'archivio corrisponde un'identità e quindi la scoperta del modello biometrico che, all'interno di una fascia di tolleranza, presenta la più alta similarità equivale

---

[175] «*Biometric verification is the comparison of a biometric sample offered at the point of transaction to a biometric template that is linked to a token (usually a PIN or access card) that the individual also presents at the point of transaction (a one-to one comparison). The use of a token in verification systems decreases processing time because a verification system compares the biometric that is presented only to the biometric template that is associated with the presented token. An identification system's flexibility with a verification system's reduced transaction time*». W. S. Coats, A. Bagdasarian, T. J. Helou, T. Lam, *The practitioner's Guide to Biometrics*, American Bar Association, Chicago, 2007, p. 6.

[176] Cfr. S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, cit., p. 135.

[177] Ne consegue che, al fine di compiere confronti aventi scopo di identificazione, le banche dati a disposizione devono contenere ingenti quantità di dati precedentemente registrati e conservati. Talvolta, le rappresentazioni digitalizzate sono confrontate con quelle archiviate nei database in cui è nota la presenza del dato del soggetto interessato (*closed-set identification*, 1:N); altre volte non si sa se il dato del soggetto si trovi all'interno del database (*open-set identification*, 1:N+1). Attualmente, in Italia, sono presenti i seguenti *database* biometrici ufficiali: 1) l'A.F.I.S.- S.S.A. (*Automated fingerprint identification system*) per le impronte digitali, integrato dal Sottosistema anagrafico S.S.A., contenente oltre le foto dei soggetti precedentemente sottoposti a fotosegnalamento, anche i dati anagrafici e le informazioni riguardanti le loro caratteristiche biometriche (cfr. il § 3.3.1.); 2) A.P.I.S. (*Automated palmprint identification system*) di raccolta delle impronte palmari; 3) la banca dati nazionale del DNA, istituita presso il Ministero dell'Interno – Dipartimento di pubblica sicurezza (cfr. il § 3.6.3).

[178] «*Biometric identification is the comparison of a biometric sample offered at the point of transaction to an entire set of stored biometric templates (a one-to-many comparison). The transaction continues if the offered sample matches a stored template. One example of biometric identification is the comparison of a criminal suspect's fingerprint to all fingerprint templates located in the FBI's Integrated Automated Fingerprint Identification System (IAFIS). IAFIS compares a suspect's fingerprint to its catalogue of millions of fingerprints from convicted criminals. Commercial transactions and government benefits system that uses a non-unique personal identification number (pin) (e.g., a telephone number) greatly reduces search times and eviscerates arguments that biometric systems are not fast enough to be used in wide scales (a one to few comparison). However, systems with non-unique PINs only work in voluntary systems, such as commercial transactions, and are not used in law enforcement, border control, or intelligence*». W. S. Coats, A. Bagdasarian, T. J. Helou, T. Lam, *The practitioner's Guide to Biometrics, American Bar Association*, cit., p. 6. Per una panoramica generale sulla distinzione fra autenticazione e identificazione si veda S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, cit., p. 134 e il Garante per la Protezione dei Dati Personali, *Linee-guida in materia di riconoscimento biometrico e firma grafometrica; Allegato A al Provvedimento del garante del 12 novembre 2014*, 2014, reperibile online www.garanteprivacy.it/documents/10160/0/ All+A+al+Provv.+513+del+12+novembre+2014+-+Linee-guida+biometria.pdf. Riassuntivamente il sistema *one-to-one* risponde alla domanda: "Sei chi dici di essere?", mentre il sistema *one-to-many* risponde al quesito: "Chi sei?".

[179] La scelta tra le due tipologie di sistemi di autenticazione e di identificazione dipende, evidentemente, dalla finalità che si intende perseguire.

tecnicamente all'identificazione del soggetto. Anche nell'ipotesi in cui i dati biometrici di un determinato soggetto non fossero contenuti nell'archivio, il confronto sarebbe utile potendosi escludere con ragionevole margine di errore che quel soggetto appartenga a quello specifico insieme[180]. Infine, la "categorizzazione" dei dati biometrici consente l'estrapolazione di tutte le informazioni potenzialmente interessanti per l'esecuzione di modelli di distribuzione di frequenza e ricerca statistica nel campo della biologia[181] e della sicurezza pubblica[182].

Ulteriore classificazione pratica da tenere presente è quella fra *sistemi di accesso fisico* e *sistemi di accesso logico*. Nei primi, il controllo biometrico viene eseguito al fine di monitorare, limitare o permettere movimenti di persone all'ingresso di aree specifiche, come locali, edifici, zone ad accesso limitato, ovvero, al fine di azionare specifiche attrezzature o oggetti[183]. Nei secondi, invece, il sistema biometrico permette l'accesso a dati o informazioni e, quindi, più specificamente, l'accertamento della titolarità del soggetto ad usufruire di una determinata risorsa informatica[184].

Proprio in ragione della specifica finalità perseguita, per l'accesso logico si utilizzano solitamente sistemi di autenticazione/verifica, mentre per l'accesso fisico anche sistemi di identificazione. Inoltre, diversi studi mostrano evidenti vantaggi pratici nell'utilizzo di un sistema di verifica/autenticazione rispetto a quello avente finalità di identificazione. Infatti, i primi risultano più rapidi e consentono un riconoscimento più preciso e accurato, mentre quelli di identificazione sono più lenti e non sempre affidabili nei risultati, dal momento che, dovendo eseguire una quantità molto elevata di confronti, richiedono un potere computazionale di gran lunga superiore ai sistemi di verifica, con una maggiore esposizione alla possibilità di errore[185]. Oltre a ciò, nel modello *one-to-many*, i dati biometrici vengono lasciati a disposizione in un unico *repository* ed è proprio tale conservazione, solitamente su ampia scala, a renderli più vulnerabili e maggiormente esposti al rischio di attacchi, cd. "*data breach*"[186],

---

[180] Cfr. S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo,* cit., p. 135.

[181] Cfr. *ex multis,* K. Mather, *Elementi di biometria*, Boringhieri, Torino, p. 25.

[182] La recente proposta di Regolamento sull'Intelligenza artificiale COM(2021) 206 final, *Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts* definisce il sistema di classificazione/categorizzazione biometrica come «*AI system for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data*». Il GRUPPO DI LAVORO – ARTICOLO 29 ha descritto il procedimento di "*biometric categorisation/segregation*" come «*the process of establishing whther the biometric data of an individual belongs to a group with some predefined characteristic in order to take a specific action*». Cfr. *Opinion 3/2012 on developments in biometric technologies*, reperibile all'indirizzo https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (visualizzato in data 5.4.2020).

[183] Per es. una cassaforte o un'automobile.

[184] Ne sono esempi, l'accesso ad un PC, ad una rete locale o aziendale, oppure l'accesso a servizi di *e-government*, *home banking* e commercio elettronico.

[185] Cfr. S. Nanavati, M. Thieme, R. Nanavati, *Biometrics. Identity verification in a networked world*, Wiley Computer Publishing, 2002, pp. 14-15, A. K. Jain, A. Ross, S. Prabhakar, An Introduction to Biometric Recognition, in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, 2004, p. 13.

[186] Per una definizione di "*data breach*" v. https://www.garanteprivacy.it/regolamentoue/databreach#:~:text=Violazioni%20di%20dati%20personali%20(Data%20Breach)

furti e riutilizzo non controllato; aumentano inoltre le possibilità di cd. falsi *match*, falsi negativi o errori[187] nelle procedure di identificazione[188].

2.5. Tipologie di errore

Come poc'anzi accennato, risulta poco probabile che due campioni di una stessa caratteristica biometrica, acquisiti in sessioni differenti, coincidano perfettamente[189]: questo può verificarsi per diverse cause, come la presenza di un rumore, cambiamenti ambientali o una cattiva interazione con l'interfaccia[190].

Uno dei temi più complessi e articolati di tutta la disciplina riguardante l'analisi biometrica forense (digitale) è rappresentato senza dubbio dal problema dell'errore, meglio denominato come "falso positivo" e "falso negativo"[191]. Più nel dettaglio, l'*output* del sistema (di solito denominato "*score*") quantifica la somiglianza fra l'*input* e il dato archiviato in precedenza nel *repository* e maggiore è il valore dello *score*, più elevata sarà la probabilità che i due campioni coincidano[192]. A tal proposito, risulta fondamentale comprendere, quindi, quali siano le misure dell'accuratezza di un determinato sistema biometrico[193]. Le principali valutazioni sulla verifica di un certo utente, eseguite su uno specifico sistema biometrico, si esprimono in termini di *False non-match rate* (FNMR)[194] e *False match rate* (FMR)[195]. Il primo si riferisce alla probabilità che due campioni coincidenti, ossia dello

&text=Una%20violazione%20di%20sicurezza%20che,trasmessi%2C%20conservati%20o%20comunque%20trattati. (visualizzato in data 4.10.2021).

[187] Cfr. il § successivo.

[188] Cfr. G. Formici, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, cit., p. 1112.

[189] Il successo di un sistema di riconoscimento dipende in gran parte dalla qualità dei campioni registrati nella banca dati (fattori endogeni o esogeni possono influire sulla corretta acquisizione del campione: per esempio nel caso del sudore di un polpastrello o della voce alterata dal raffreddore).

[190] La superficie del dispositivo attraverso il quale il dato biofisico è acquisito.

[191] Cfr. M. Mendola, *Aspetti informatici delle prove biometriche. Il problema dei "Falsi positivi"*, in *Psicologia e Giustizia*, Anno 14, numero 1, 2013.

[192] Cfr. K. Delac, M. Grgic, *A survey of biometric recognition methods*, in *46th International Symposium Electronics in Marine*, ELMAR-2004, 2004, Zadar, Croatia, p. 10.

[193] Cfr. B. Lavanya, H. Inbarani, *A Survey of Biometric Techniques*, in *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, 7, 2015, p. 708.

[194] O in modalità di confront 1:1, cd. "*false rejection rate*".

[195] Detto anche *false match probability* o, in modalità di confronto 1:1, cd. "*false acceptance rate*". Invero, un ulteriore parametro fondamentale di un sistema biometrico è rappresentato dal cd. *Equal Error Rate* (EER), il cui valore è rappresentato dal punto di intersezione fra le curve del FMR e FNMR e costituisce una misura dell'accuratezza globale di un sistema biometrico. Cfr. COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, 26.11.2010.
«*A biometric verification system makes two types of errors: 1) mistaking biometric measurements from two different persons to be from the same person (called false match) and 2) mistaking two biometric measurements from the same person to be from two different persons (called false nonmatch). These two types of errors are often termed as false accept and false reject, respectively. There is a tradeoff between false match rate (FMR) and false non match rate (FNMR) in every biometric system*». A. K. Jain, A. Ross, S. Prabhakar, *An Introduction to Biometric Recognition*, in *IEEE Transactions on Circuits and Systems for Video Technology*, vol.14, no. 1, 2004, p. 6.

stesso tratto biometrico e acquisiti dallo stesso utente, siano dichiarati erroneamente come provenienti da due individui diversi[196]. Il secondo valore, invece, indica la probabilità attesa che due campioni appartenenti a due individui diversi siano riconosciuti come coincidenti[197]. La maggior parte dei casi in cui si verifica un FNMR è dovuta ad una cattiva interazione dell'utente con il sensore del sistema e può essere facilmente risolta permettendo al soggetto di presentare nuovamente l'*input*. L'ipotesi di FMR, invece, si riferisce ai tentativi di soggetti che, pur non essendo autorizzati, ottengono l'accesso ad un sistema, portando a compimento attacchi di sicurezza. Come poc'anzi accennato, si tratta di misure applicabili ai sistemi di verifica (1:1) che, tramite alcune semplificazioni di calcolo, possono essere utilizzati come parametro anche per i sistemi biometrici con finalità identificativa (1:N, 1:N+1)[198]. I livelli di accuratezza di un sistema biometrico dipendono in larga parte dalla tipologia di applicazione che si intende effettuare. Ai fini che qui interessano, uno dei punti più critici è rappresentato dal tasso FNMR (e non dal FMR): ciò significa che l'identificazione di un soggetto ignoto costituisce un obiettivo tanto importante che, talvolta, si corre il rischio di esaminare numeri anche molto elevati di corrispondenze già potenzialmente errate generate dal sistema biometrico stesso[199].

---

[196] La formula matematica del valore di FNMR si trova espressa come FNMR (h)=1 – $\int_{s=-\infty}^{h} pm(s)\, ds$. Più nel dettaglio, «*FNMR is the rate that the decision is made that I does not match T, while I and T do in fact come from the same individual, where pm(s) is the match distribution between two samples as a function of the score s*». A. I. Awad, A. E. Hassanien, *Impact of Some Biometric Modalities on Forensic Science*, in AA.VV., *Computational Intelligence in Digital Forensics, in Forensic Investigation and Applications, Studies in Computational Intelligence* 555, (a cura di) A. K. Muda et al., Springer International Publishing Switzerland 2014. La percentuale si trova anche indicata con la dicitura FRR ossia *False Rejection Rate.*

[197] Per esempio, con riferimento all'utilizzo di sistemi biometrici con finalità identificativa «un "falso positivo" potrebbe verificarsi a causa di un errore nella raccolta o nella manipolazione reiterata dei dati genetici, nell'interpretazione distorta dei risultati dei *tests*, oppure, nell'erronea segnalazione dei risultati di prova». M. Mendola, *Aspetti informatici delle prove biometriche. Il problema dei "Falsi positivi"*, in *Psicologia e Giustizia*, Anno 14, numero 1, 2013. Quando si considera la più specifica prova del Dna, un ulteriore indice da tenere in considerazione è la cd. *random match probability* (RMP) che può essere definita come la probabilità che una persona scelta a caso abbia lo stesso profilo del Dna rispetto ad un profilo prefissato. Sul punto si v. M. Bramanti, *Valutazioni probabilistiche sui riscontri del DNA a scopo di identificazione criminale*, in *La Matematica nella Società e nella Cultura - Rivista dell'Unione Matematica Italiana*, I, vol.II, n. 3, 2009, p. 452. La formula matematica del valore di FMR è FMR (h)=1 – $\int_{s=h}^{\infty} p_n(s) ds$, ove, «*FMR is the rate that the decision is made that I matches T, while in fact I and T come from two different individuals where pn(s) is the non-match distribution between two samples as a function of the similarity score s*». A. I. Awad, A. E. Hassanien, *Impact of Some Biometric Modalities on Forensic Science*, in AA.VV., *Computational Intelligence in Digital Forensics, in Forensic Investigation and Applications*, (a cura di) A.K. Muda et al., Springer International Publishing, Switzerland, 2014.

[198] «*The accuracy of a biometric system in the identification mode can be inferred using the system accuracy in the verification mode under simplifying assumptions*». A.K. Jain, A. Ross, S. Prabhakar, *An Introduction to Biometric Recognition*, in *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, no. 1, 2004, p. 7. Cfr. anche v. D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, *FVC2002: Fingerprint verification competition*, in *Proc. Int. Conf. Pattern Recognition (ICPR)*, Quebec City, QC, Canada, 2002, pp. 744-747 e J. L. Wayman, *Fundamentals of biometric authentication technologies*, *Int. J. Image Graphics*, vol. 1, no. 1, 2001, pp. 93-113.

[199] Sul punto, è interessante richiamare il seguente esempio: «*in negative recognition applications such as employee background checking and preventing terrorists from boarding airplanes, the personal recognition is required to be performed in the identification mode. As mentioned earlier, achieving the same accuracy in an identification system as in a verification system is a much harder problem due to the large number of comparisons that are required to be performed. Consider that airport authorities are looking for the FBI's 100 most wanted criminals (database size of 100) and the state-of-the-art fingerprint verification system*

Pertanto, laddove si renda necessario fare uso nel processo di dati biometrici, in funzione di prova dei fatti oggetto del procedimento, occorre tenere a mente sia l'indice di *false non match rate*, sia il *false match rate*[200]. A prescindere dall'ordinamento giuridico di riferimento, quando si introduce una prova biometrica in un procedimento penale, la tendenza dei consulenti è quella di indicare i dati statistici sulla probabilità di una determinata coincidenza di un campione (cd. *score* dell'*output*) rispetto al valore effettivo della percentuale di errore[201]. Come si vedrà meglio *infra*[202], ciò ha notevoli implicazioni pratiche, in quanto riguarda direttamente l'accettazione del risultato da parte della comunità scientifica di riferimento rispetto all'accertamento dei fatti oggetto del procedimento[203].

---

operates at 1% FNMR and 0.001% FMR, i.e., if this system was deployed as a verification system, the system would fail to match the correct users 1% of the time and erroneously verify wrong users 0.001% of the time. Let us consider the outcome of the same system when deployed as an identification system. While the identification will still be 1%, the identification will be. This means that, while the system has a 99% chance of catching a criminal, it will produce large number of false alarms (e.g., assuming that 200 000 people may use a major U.S. airport in a day, the system will produce 200 false alarms!). Further, if faces are used instead of fingerprints for the identification (face recognition may be preferred for an airport application because faces can be acquired covertly), the number of misses and false alarms will be considerably higher, given the rather poor accuracy of face identification systems, especially in environments with cluttered background and varying lighting conditions. Although multimodal biometric systems can significantly improve the identification accuracy, exclusively relying on automatic biometric systems for negative identification may be unfeasible. Traditional personal recognition tools such as passwords and PINs are not at all useful for negative recognition applications. While biometric systems may not yet be extremely accurate to support large-scale identification applications, they are the only choice for negative recognition applications. Further, if operated in a semi-automatic mode where a human expert examines all the alarms generated by the system for the final decision, biometric systems can be quite effective. For example, if 100 airport security agents are required to manually match every person at an airport against the FBI's 100 most wanted, only five agents may be required to take a closer look at the 200 alarms generated daily by the biometric system. We need to understand that, in such semi-automatic applications, the biometric system only generates an alarm that calls for a closer (manual) examination of the individual and an alarm does not directly translate into catching a terrorist. In fact, the tradeoff between the FMR and FNMR rates in a biometric system is no different from that in any detection system, including the metal detectors already in use at all the airports. Other negative recognition applications such as background checks and forensic criminal identification are also expected to operate in semi-automatic mode and their use follows a similar cost-benefit analysis. For example, in a latent search, an automatic fingerprint identification system (AFIS) is typically used by law enforcement agencies only to narrow down the number of fingerprint matches to be performed by a human expert from a few million to a few hundred. A forensic expert always makes the final decision. In our opinion, use of biometrics in negative recognition applications does not infringe upon the civil liberties of individuals since, if you are not in the "criminal database" already, the recognition system does not keep a record of you (does not remember you). However, appropriate legislation is required to protect the abuse of such systems». A. K. Jain, A. Ross, S. Prabhakar, *An Introduction to Biometric Recognition*, in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, 2004, p. 13.

[200] Con particolare riferimento alla prova del Dna, si v. *ex multis* J. J. Koehler, A. Chia, S. Lindsey, *The Random match probability in DNA evidence: Irrelevant and Prejudicial*, in *Jurimetrics Journal*, 1995, pp. 201-218.

[201] «(…) *the probability of selecting an unrelated individual at random from the population having a DNA profile matching [the defendant's] [is] approximately 1 in 351,200 blacks and approximately 1 in 572,000 Caucasians. But juries rarely hear statistics on the frequency or probability of false positives*». W. C. Thompson, F. Taroni, C. G. G. Aitken, *How the Probability of a False Positive Affects the Value of DNA Evidence*, in *J. Forensic Science*, 2003, Vol. 48, no. 1, pp. 1-2.

[202] Cfr. il capitolo III.

[203] In tal senso, come si approfondirà meglio *infra*, v. *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579. Come noto, la pronuncia è giunta a definire gli elementi indispensabili nella "costruzione" della prova scientifica nel processo penale (*in primis* negli USA, poi diffusa e recepita da molti altri ordinamenti giuridici nazionali). I punti cardine della sentenza sono: a) la verificabilità del metodo (una teoria è scientifica solo se controllabile mediante esperimenti); b) la falsificabilità (sottoporsi a tentativi di smentita ed individuare con certezza i limiti della stessa teoria); c) la conoscenza del tasso di errore (è necessario comunicare al giudice l'ipotesi di errore calcolata e consentire al giudice stesso il ruolo di *gatekeeper*, o meglio di "custode" della prova scientifica); d) la sottoposizione al controllo della comunità scientifica (consente un controllo capillare da parte degli esperti

3. Le tecnologie biometriche. Cenni sul differente potenziale carattere distintivo o tipico dei tratti biometrici

A questo punto, dopo aver esaminato alcuni dei caratteri più salienti e comuni ai diversi sistemi di riconoscimento biometrici, è doveroso soffermarsi, seppure per brevi cenni, sull'analisi delle tecniche attualmente più diffuse a fini sia privatistici che pubblici. Tale approccio consentirà non solo di comprendere il procedimento di identificazione in relazione ai vari sistemi, ma anche di evidenziare quali siano le principali problematiche collegate a ciascuno di essi, in base ad alcuni parametri fissi (cfr. il § 1.1), al fine di individuare il differente potenziale identificativo delle diverse tecniche[204]. Peraltro, giova ricordare che alcune di queste tecniche possono essere utilizzate sia da sole che in combinazione con altre tipologie di sistemi biometrici (cd. "*multimodal biometrics*")[205].

3.1. Le impronte digitali

L'identificazione delle impronte digitali costituisce una delle tecniche maggiormente utilizzate in biometria forense[206]. Fin dalla fine del XIX secolo[207], infatti, l'analisi delle impronte digitali è stata

del settore tramite la pubblicazione delle tesi scientifiche nelle riviste specializzate). Cfr. M. Mendola, *Aspetti informatici delle prove biometriche. Il problema dei "Falsi positivi"*, in *Psicologia e Giustizia*, Anno 14, numero 1, 2013.

[204] Sul punto, M. Biral, *L'Identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, in *Riv. It. di Dir. e Proc. Pen*., fasc.4, 2015, p. 1842: «gli indicatori che tale scienza impiega sono eterogenei: accanto ai segni immutabili della persona (il Dna, per esempio), che presentano una spiccata capacità "identificativa", ve ne sono anche altri, i quali, non essendo né irripetibili né costanti nel tempo (si pensi ai parametri comportamentali, quali l'andatura e la grafia), risultano meno affidabili». V. anche P. Rivello, Tecniche scientifiche e processo penale, in *Cass. pen*., Fasc. 4, 2013, p. 1691 e ss.

[205] Il campo della biometria multimodale non ha ancora trovato compiuta applicazione in ambito giudiziario e pertanto non è oggetto di trattazione nella presente ricerca.

[206] Cfr. S. Smyth, *Biometrics, surveillance and the law. Societies of restricted access, discipline and control, Routledge*, New York, 2019, pp. 24 e ss.

[207] Le basi della moderna identificazione dattiloscopica sono state sviluppate da Francis Galton (Sparkbrook, 16.2.1822 – Haslemere, 17.1.1911) e Edward Henry (Londra, 26.7.1850 – Ascot, 19.2.1931) verso la fine dell'Ottocento, ma i primi studi risalgono già ai primi anni del '700. Inizialmente la classificazione delle impronte si basava sul metodo di Henry, il quale si concentrava sullo studio delle forme di particolari punti trovati su un'impronta (per es. i punti di *loop*, *whorl*, etc.). Successivamente è stato adottato il metodo di Galton che si basava su differenti caratteristiche delle impronte, ossia le terminazioni e le biforcazioni: lo studioso per la prima volta ha decretato i principi fondamentali in materia, tra cui l'immutabilità delle impronte nel corso della vita, la variabilità nonché la classificabilità dei tipi principali, e infine, l'unicità dei caratteri. Il metodo di Galton è stato ripreso e perfezionato da Giovanni Gasti, criminologo e inventore del metodo di classificazione delle impronte digitali utilizzato dalla Scuola Italiana di Polizia Scientifica (Castellazzo Bormida, 30.1.1869 – Roma, 11.4.1939). Solo intorno al 1950 sono stati sviluppati i primi sistemi automatici per il riconoscimento delle impronte digitali da parte del *Federal Bureau of Investigation* (F.B.I.), ente investigativo di polizia federale del Dipartimento di Giustizia degli Stati Uniti (DOJ) in collaborazione con la *Rockwell International Corporation* e il *Cornell Aeronautical Laboratory*. I sistemi sviluppati successivamente sono stati adottati in differenti contesti e gli Organi di Polizia, affiancati da Enti Governativi e Privati, hanno perso la prerogativa di unico destinatario di queste tecnologie. Infatti, i primi sistemi commerciali destinati ad applicazioni non forensi e non governative sono stati sviluppati a partire dagli anni '80 del secolo scorso. Cfr. A. Giuliano, *Dal pensiero di Lombroso all'impronta digitale. Passato e presente del metodo più efficiente, pratico e rapido d'identificazione personale*, Edizioni libreria Cortina, Torino, 2012, pp. 21 e ss.

utilizzata per l'identificazione personale[208]. La dattiloscopia ha da sempre rappresentato uno dei sistemi di riconoscimento personale più significativi sia nella fase delle indagini preliminari sia in quella del giudizio vero e proprio. Trattasi di una disciplina considerata altamente affidabile e caratterizzata da un significativo grado di *immutabilità, univocità*[209] e *classificabilità* (cfr. il § 1.1)[210].

Gli elementi anatomici delle impronte digitali, che si sogliono prendere in considerazione a fini identificativi, sono costituiti da un insieme di linee rette cd. *Ridge Line* o Creste[211], che scorrono per lo più in fasci paralleli e, intersecandosi, formano un disegno denominato *Ridge Pattern*[212]. Analizzando la struttura delle creste si possono notare alcune regioni in cui esse assumono andamenti particolari, come, per esempio, le curvature accentuate, le terminazioni o le biforcazioni[213]. A fini identificativi, particolarmente rilevanti risultano le cd. micro-singolarità[214], anche denominate

[208] G. Iovane, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza*, Aracne editore, Roma, 2008, pp. 193 e ss.

[209] Questa affermazione è valida anche per i gemelli omozigoti.

[210] L'utilizzo delle impronte digitali per le due diverse finalità di "autenticazione" e "identificazione" richiede tecniche di confronto differenti, in quanto, come visto *supra* al § 2.4, nel primo caso si tratta di paragonare due sole impronte, mentre nel secondo occorre un confronto di tipo 1:N o 1:N+1, ossia il campione di ingresso deve essere trovato fra un numero solitamente molto elevato di impronte. Per la modalità di "verifica", diversamente che per l'"identificazione", non si pone l'obbligo di implementare algoritmi efficienti di confronto. Per tale ragione, gran parte dei sistemi *one to many* è basato sull'utilizzo di algoritmi che limitano il tempo di confronto fra i modelli elettronici e sono in grado di riconoscere immagini affette da "rumori". Cfr. G. Iovane, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza*, cit., p. 193. La Cassazione già negli anni '80 del secolo scorso ha riconosciuto alla comparazione di impronte digitali a fini identificativi piena garanzia di attendibilità senza bisogno di ulteriori elementi sussidiari di conferma [Cfr. *ex multis*, Cass. pen., Sez. IV, 2.2.1989 n. 4254 in *CED Cass* n. 180856; Cass. pen., Sez. II, 13.4.1988 n. 1483 in *CED Cass* n. 180364; Cass. pen., Sez. II 8.5.1986 n. 11410 in *CED Cass* n. 174046]. Tuttavia, negli ultimi anni sono stati diffusi studi che hanno evidenziato alcune criticità emergenti dall'utilizzo di tali tracce a fini identificativi e giudiziari. Uno di questi si deve all'*American Association for the Advancment of Science* (AAAS), la più importante associazione a livello mondiale, dedita al progresso della scienza (disponibile qui: https://www.aaas.org/news/fingerprint-source-identity-lacks-scientific-basis-legal-certainty, ultima visualizzazione in data 24.2.2021). Sui principi fondamentali in tema di identificazione personale ottenuta a mezzo di impronte digitali, v. AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienza, logica*, (a cura di) D. Curtotti, L. Saravo, Giappichelli, Torino, 2019, pp. 648 e ss.

[211] «La pelle del palmo delle mani, della pianta dei piedi e delle falangi delle dita è caratterizzata dalla presenza di creste e di solchi (dermatoglifi, in anatomia) che si dispongono regolarmente le une a fianco delle altre. Nell'insieme appaiono come dei flussi che formano dei vortici e danno luogo a caratteristici disegni papillari che sono alla base dei vari sistemi di classificazione». D. Curtotti, L. Saravo, *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienza, logica*, Giappichelli, Torino, 2019, pp. 648 e ss. Inoltre l'andamento delle *ridge lines* può essere descritto dalla cd. "immagine direzionale", che è una matrice i cui elementi sono vettori non orientati ottenuti tramite la sovrapposizione di una griglia a maglia quadrata all'immagine dell'impronta. Ogni vettore è posto in un nodo della griglia e ha direzione parallela a quella della *flow line* che attraversa il medesimo. Tali vettori, in particolare, denotano l'orientamento della tangente alle *ridge line* in corrispondenza dei nodi della griglia.

[212] Oppure cd. *global pattern configuration*. «Nell'analisi della struttura delle impronte digitali ricorre anche il termine *Flow-Line* o Linea di Flusso: si tratta di un'ipotetica linea che corre parallelamente ad un insieme di creste contigue. La *Flow-Line* non ha una controparte fisica e la sua determinazione non è univoca, ma dipende dalle ipotesi fatte al momento in cui la si localizza. Con *Ridge-Count* (AB) si intende il numero di *ridge line* intersecate dal segmento di estremi A e B, punti generalmente situati in zone facilmente identificabili dell'impronta, come il centro ed una regione singolare». G. Iovane, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza*, cit., p. 194.

[213] Tali zone, denominate "singolarità" o "regioni singolari", sono riconducibili a tre categorie distinte: a) *Core* (o *Loop*): caratterizzate da un insieme di creste che hanno un andamento a forma di *U*; b) *Whorl*: caratterizzata da una struttura ad *O*; c) *Delta*: caratterizzata da creste che delineano una struttura a forma di delta per l'appunto.

[214] Cd. *local ridges and furrow details*.

"minuzie", ovvero, "caratteristiche di Galton"[215]. In generale, le impronte papillari, siano esse digitali, palmari o plantari, consistono nella riproduzione di creste e solchi presenti sui polpastrelli, sul palmo delle mani e sulla pianta dei piedi[216].

La maggior parte delle tecniche di *matching* delle impronte digitali, basate sulle minuzie[217], presuppone una prima fase di estrazione delle stesse dalle impronte e un successivo confronto dei due insiemi di minuzie estratti[218]. Grazie al progredire dello sviluppo tecnologico[219], i sistemi di acquisizione delle impronte digitali si basano su tecniche opto-elettroniche, costituite da un prisma ottico, che permette di eseguire un'immediata scansione dell'impronta e conseguente trasformazione in un'immagine digitale ed eventualmente in un modello elettronico[220]. Secondo la maggioranza delle interpretazioni offerte dalla giurisprudenza, l'individuazione e il rilevamento delle impronte

[215] Esse rappresentano i punti in cui si verifica un comportamento anomalo delle cd. *ridge line* e possono essere interruzioni, uncini, interlinee, incroci, tratti, punti, isolotti, occhielli, occhi e intrecci. L'origine delle impronte e, più in particolare, delle minuzie si ha in fase intrauterina. La parte centrale dell'impronta, invece, dove sono normalmente dislocate le singolarità è detta *pattern area* ed è delimitata da due linee principali, denominate *type line*, che sono individuabili come le due linee più interne che la separano dal resto dell'impronta. Le singolarità, insieme alla forma e alla direzione delle *ridge line* e della *pattern area*, costituiscono le macro-caratteristiche dell'impronta su cui si basa la maggior parte dei sistemi di classificazione delle impronte digitali. Cfr. AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienza, logica,* cit., p. 648.

[216] Cfr. AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienza, logica*, cit., p. 649.

[217] Cfr. il § 2.3.

[218] Più nel dettaglio, le impronte papillari possono essere latenti, costituite da una mistura non visibile di secrezioni naturali distribuita sulla superficie, modellate o per spostamento, quando è avvenuto un contatto con sostanze malleabili, come cera o resina, e infine, visibili, in cui le creste sono composte da materiale vario percettibile alla vista, come il grasso, l'inchiostro, il sangue ed altro ancora. Possono essere positive, se nel contatto avviene un lascito di materiale, e negative, qualora avvenga un'asportazione del materiale già presente sulla superficie. In particolare, in ogni sopralluogo, la ricerca di tracce latenti costituisce uno dei principali impegni da affrontare. Per l'identificazione personale occorre procedere con il metodo A.C.E.-V.: ad una prima fase di analisi, seguono il confronto e la valutazione. Il procedimento termina con la verifica. Le impronte sono suddivise in otto categorie principali, in base al numero e alla posizione delle singolarità. Tale classificazione risulta utile per velocizzare operazioni di ricerca di impronte su database di grosse dimensioni. Le classi di impronte sono le seguenti: a) *ARCH* o impronta ad arco semplice: impronte in cui le creste entrano da un lato, crescono verso il centro e scendono per poi uscire dal lato opposto; b) *TENTED ARCH* o impronta ad arco a tenda: impronte che hanno lo stesso andamento di quelle ad arco semplice, ma le creste formano un angolo o una piega al centro con la presenza di un delta; c) *RIGHT LOOP* o impronta ad occhiello radiale: come le precedenti, ma piegate dal lato opposto; d) *WHORL* o impronta a spirale semplice: impronte con almeno due delta e una figura chiusa (circolare, ellittica, o a spirale) centrale; e) *DOUBLE LOOP* o impronta a doppio occhiello: impronte con due delta e due loop distinti accavallati; f) impronta a occhiello centrale a sacca: mostra al centro un occhiello che ricorda una sacca; g) impronta casuale: il cui *pattern* non è ascrivibile a specifiche forme. Lo studio dei dati raccolti può essere suddiviso in diverse categorie, tra le quali vi sono l'*approccio statistico* (in cui sono analizzati i dati oggettivi, in particolare, i vettori, direttamente dai campi d'immagine dell'impronta) e l'*approccio strutturale* che consente di individuare le specificità comparando i singoli campioni rilevanti. Cfr. AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienza, logica*, cit. pp. 650 e ss.

[219] 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.

[220] 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).

dattiloscopico-papillari rientrano nell'alveo dell'istituto di cui all'art. 354 co. 2 c.p.p.[221] ovvero, a fini identificativi, nelle attività disciplinate dall'art. 349 co. 2 c.p.p., eseguibili dalla polizia giudiziaria[222].

Il sistema di comparazione tra il campione estratto e quello digitalizzato, ottenuto per essere conservato nei database, costituisce il principale punto di forza nella disciplina dattiloscopica e, contestualmente, la problematica più complessa[223]: i vantaggi nell'utilizzo di strumentazioni automatiche o semi-automatiche si manifestano in termini di accuratezza, velocità e disponibilità immediata di dati. Ciò nonostante, emergono alcune difficoltà: certune legate alla necessità che le apparecchiature dispongano di notevoli capacità di calcolo (oggi parzialmente superate, grazie al progresso scientifico-tecnologico), altre riguardano le già accennate criticità legate ai falsi positivi[224]. Risultano comunque tecnologie molto utili per operare grandi "scremature" di dati giacché risulta sempre necessario l'intervento umano[225]: prima, al fine di evidenziare quali sono i dettagli da ricercare nei database, e poi per analizzare e confermare i candidati che il sistema offre[226]. Giova sottolineare che il risultato di una comparazione fra modelli elettronici biometrici eseguita automaticamente da un software collegato ad una banca dati (1:N, 1:N+1), è sempre soggetto ad una verifica da parte di un

[221] Cass. pen., Sez. II, 25.6.2003, n. 23711 in *CED Cass* n. 225170; Cass. pen., Sez. II, 7.5.1999, n. 5779 in *CED Cass* n. 213311.

[222] In tal caso infatti gli accertamenti compiuti dalla p.g. consistono nel rilevamento delle impronte su oggetti e nel raffronto delle stesse con quelle di un soggetto. Attività che non richiedono particolari cognizioni tecniche ma solo un accertamento di dati oggettivi che possono essere valutati dal giudice senza dover ricorrere al sapere scientifico di un consulente tecnico. AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze, logica*, cit., p. 77. In dottrina e in giurisprudenza, è emersa anche l'interpretazione che distingue gli "accertamenti", caratterizzati da valutazione e studio di elementi, dai "rilievi", ossia mere osservazioni o acquisizioni di dati materiali. I primi rientrerebbero nell'alveo di applicazione dell'art. 359 c.p.p. o, in caso di irripetibilità, dell'art. 360 c.p.p.; per i rilievi, invece, sarebbe possibile procedere ai sensi dell'art. 354 c.p.p. Cfr. A. Amato, G. Flora, C. Valbonesi, *Scienza, diritto e processo penale nell'era del rischio*, Giappichelli, Torino, 2019, p. 295.

[223] Anche l'attività di comparazione delle impronte digitali rientra fra le operazioni eseguibili dalla polizia giudiziaria ai sensi dell'art. 354 o dell'art. 349 co. 2 c.p.p.

[224] Cfr. il § 2.5 e sia consentito il rinvio a E. Sacchetto, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2/2019. Il report pubblicato dall'*American Association for the Advanment of Science* (AAAS), tra le diverse criticità rilevate rispetto all'utilizzo delle impronte digitali a fini giudiziari, ha mostrato da un lato l'estrema accuratezza dei sistemi automatizzati per la ricerca di impronte digitali, dall'altra la poca precisione degli stessi con riferimento ai frammenti di impronte latenti.

[225] In Italia, i software automatizzati di comparazione possono essere utilizzati solo come ausilio per il dattiloscopista. L'attribuzione dell'identità viene sempre eseguita dal dattiloscopista e mai dalla macchina. Cfr. A. Amato, G. Flora, C. Valbonesi, *Scienza, diritto e processo penale nell'era del rischio*, cit., p. 293.

[226] Cfr. A. Amato, G. Flora, C. Valbonesi, *Scienza, diritto e processo penale nell'era del rischio*, cit., p. 283.

operatore esperto del livello di compatibilità fra le due diverse impronte[227]. Pertanto, lo strumento automatico di riconoscimento costituisce solamente un ausilio per il dattiloscopista[228].

Quanto alla fase di valutazione delle impronte, il criterio di riferimento è ancora oggi oggetto di numerosi dibattiti e confronti fra gli esperti[229]. Seppur per brevi cenni, si intende dar conto di due posizioni distinte sul tema, rispettivamente individuate con un approccio numerico e non numerico[230]. Nel primo caso, la valutazione si basa sul raggiungimento di uno standard soglia, ossia un numero minimo di minuzie che devono poter essere individuate in un'impronta, per potersi esprimere in termini di certezza di un'unica provenienza[231]. La maggior parte dei Paesi europei risulta in linea con tale approccio[232], anche se poi ciascuno interpreta diversamente la soglia di tale standard[233].

---

[227] Questo perché le condizioni di acquisizione delle impronte digitali presenti nella banca dati A.F.I.S. (Cfr. *infra* il § 3.3.1.) sono sempre differenti (per es. la luce, la posizione, la qualità dell'immagine etc.). Lo stesso vale per il riconoscimento facciale come si vedrà meglio *infra* al § 3.3. La verifica da parte dell'operatore esperto costituisce certamente una garanzia di affidabilità della comparazione fra le impronte. Tuttavia, il report dell'AAAS parla di "*bias* cognitivo" derivante dal contesto complessivo delle indagini a cui i dattiloscopisti sono costantemente esposti: la particolare vicinanza agli organi d'accusa e la conoscenza di informazioni investigative non strettamente necessarie possono condurre a conclusioni errate. A tal proposito, sono necessari interventi di cd. *debiasing* cognitivo, con l'adozione di pratiche che minimizzino il più possibile questi fenomeni, al fine di rendere il giudizio del dattiloscopista il più imparziale possibile. Cfr. A. Amato, G. Flora, C. Valbonesi, *Scienza, diritto e processo penale nell'era del rischio*, cit., p. 283.

[228] Cfr. A. Amato, G. Flora, C. Valbonesi, *Scienza, diritto e processo penale nell'era del rischio*, cit., p. 292.

[229] Cfr. AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienza, logica*, cit., p. 651.

[230] Cd. *empirical standard approach* e *holistic quality approach*.

[231] Tale criterio risale alla formula empirica creata all'inizio del '900 dal matematico francese Victor Balthazard (1850-1931). Per la prima volta, lo studioso ha ipotizzato che «fra due impronte si sarebbero potuti riscontrare appena diciassette punti di corrispondenza su una serie di 18.179.869.184 esemplari. In pratica, una possibilità su decine di miliardi che un frammento di impronta contenente 17 contrassegni caratteristici possa essere stato depositato da una persona diversa da quella a cui viene attribuito». A. Scarscella, *Condizioni dell'efficacia probatoria nell'indagine dattiloscopica*, in *Diritto Penale e Processo*, 2012, fasc. 1, 68, p. 2.

[232] La Corte di cassazione ha da sempre adottato tale criterio. Inizialmente, la Cass. pen., Sez. II, n. 2559, 1959, in AA.VV., *La prova tecnica nel processo penale. Aspetto pratico scientifici*, (a cura di) A. Barbaro, A. La Marca, E. Nobile, P. Romeo, Editore Key, Firenze, 2016, p. 314, ha per la prima volta affermato il principio secondo cui le impronte digitali offrono piena garanzia di attendibilità, posto che dalle indagini emerga l'esistenza di 16-17 punti caratteristici uguali per forma e posizione. La sentenza della Cassazione affonda le radici della propria posizione sul calcolo statistico effettuato da Balthazard, per cui, di fronte a diciassette minuzie in comune, la probabilità che l'impronta appartenga a un soggetto diverso è estremamente bassa (conf. Cass. pen., Sez. II, 8.6.1978 n. 13771 in *CED Cass* n. 140367; Cass. pen., Sez. II, 5.7.1985 n. 10567 in *CED Cass* n. 171037; Cass. pen., Sez. II, 2.04.2008 n. 16356 in *CED Cass* n. 239781; Cass. pen., Sez. V, 26.02.2010 n. 12792 in *CED Cass* n. 246901). Quanto statuito dalla succitata pronuncia ha condizionato in modo piuttosto rilevante il valore probatorio da attribuire alla prova dattiloscopica. A partire dagli anni '70, diverse organizzazioni internazionali hanno constatato come non esistano basi valide per esigere un numero minimo di minuzie comuni a due impronte per stabilire un'identificazione positiva (*International Association for Identification* - I.A.I., 1°.8.1973). Nonostante ciò, la giurisprudenza è rimasta granitica sul punto. Si intende tuttavia dare conto di una pronuncia isolata, Cass. pen., Sez. I, 15.3.2011, n. 17424 in *CED Cass* n. 250323 (con nota di A. Scarcella in *Dir. Pen. e Processo*, 2012, 1, 68), in cui la Corte ha ritenuto di abbandonare la logica dell'automatismo probatorio conseguente alla assiomatica corrispondenza dei canonici 16-17 punti, affermando che quest'ultima può assumere maggiore o minore valenza indiziaria a seconda della natura dei punti di corrispondenza (semplici o complessi), ovvero dei contesti di tempo e di luogo in cui la traccia ignota è stata lasciata, in riferimento ai potenziali soggetti cui riferirla. Cfr. A. Scarcella, *Condizioni dell'efficacia probatoria dell'indagine dattiloscopica*, in *Dir. Pen. e Processo*, 2012, 1, 68.

[233] «In particolare, alcuni Paesi sono tuttora in linea con discutibili e rigidi standard numerici mentre altri hanno scelto di adeguare il limite alla qualità e particolarità delle minuzie». AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienza, logica*, cit., p. 651.

Nel secondo, invece - cd. "approccio olistico" - la valutazione succede all'analisi di tutte le informazioni rilevabili in un'impronta in base alle caratteristiche di primo, secondo e terzo livello[234]. Entrambi i criteri prevedono una soluzione "chiusa", senza alternative all'esclusione o all'individuazione esatta della fonte della traccia. Entrambi i criteri attivano veri e propri automatismi dai quali deducono l'assoluta attendibilità della prova. Tale modo di porsi nei confronti di una prova scientifica - quale quella dattiloscopica - rappresenta una sorta di "appiattimento" del dibattito in materia[235]. Infatti, la prassi mostra come, talvolta, sia importante un approccio che si esprima in termini probabilistici[236]: il numero delle informazioni rilevabili non è sempre così elevato da raggiungere e superare quel limite di certezza dato dallo standard numerico o, nell'altro caso, dall'intima convinzione "*aldilà di ogni ragionevole dubbio*" dell'unicità delle caratteristiche e della provenienza dell'impronta. Anche in una traccia cd. "indefinibile"[237], è possibile ricavare informazioni di primo o di secondo livello, importanti da valutare nel contesto di un'indagine. Tuttavia, i criteri di interpretazione delle prove scientifiche impongono comunque di valutare il peso di tale incertezza, anche con riferimento alle impronte papillari[238]. Ne consegue, dunque, che i criteri di individuazione della provenienza di una traccia necessitano anche di un processo logico induttivo, di tipo probabilistico, da cui è possibile valutare l'eventuale *error rate*[239].

3.2. Il riconoscimento della geometria della mano e l'impronta palmare

Il sistema di riconoscimento della geometria della mano misura le caratteristiche fisico-geometriche della stessa: la forma, la larghezza, la lunghezza delle dita e delle nocche nonchè lo spessore del palmo (o dita)[240]. La tecnologia più diffusa impiega una telecamera per catturare alcune misure geometriche comprensive di lunghezze, distanze ed angoli (cd. *silhouette*)[241]. Nonostante tale

[234] Adottano tale criterio i Paesi che hanno aderito all'IAI (*International Association for Identification*). Cfr. J. Almog, E. Springer, M. Yiśra'el. *Proceedings of the International Symposium on Fingerprint Detection and Identification,* 1995, Neurim-Israel, ove emerge chiaramente la posizione di Israele sul tema: «*No scientific basis exists for requiring that a predetermined minimum number of friction ridge features be present in two impressions in order to establish a positive identification*».

[235] Cfr. A. Amato, G. Flora, C. Valbonesi, *Scienza, diritto e processo penale nell'era del rischio*, cit., p. 295.

[236] Certamente, si considera «fuori discussione che il dato statistico possa legittimamente rientrare in determinati casi nel patrimonio di conoscenze a disposizione del giudice". Cfr. F. Caprioli, *L'accertamento della responsabilità penale "oltre ogni ragionevole dubbio"*, in *Riv. it. dir. proc. pen*., 2009.

[237] Denominata in tal modo per indicare una valutazione al di sotto degli standard enunciati *supra*.

[238] Cfr. AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienza, logica*, cit., p. 652.

[239] Cfr. AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienza, logica*, cit., p. 652.

[240] Si parla anche di cd. "impronta palmare".

[241] Sia consentito il riferimento a E. Sacchetto, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2/2019, p. 470.

sistema, introdotto intorno agli anni Settanta del secolo scorso, sia utilizzato ormai da diversi anni, risulta ancora piuttosto dibattuto l'aspetto dell'*unicità* della geometria della mano[242].

Alcuni studiosi, infatti, sostengono che la geometria della mano non presenti elementi *univoci* tali da permettere il riconoscimento un individuo[243]. Anche dal punto di vista del parametro dell'*invarianza*, la caratteristica biometrica è oggetto di discussione fra gli esperti, poiché possono essere molteplici i cambiamenti nel tempo[244]. Per tale ragione, il sistema viene utilizzato soprattutto per le autenticazioni, ossia in modalità di "verifica"[245].

Più attendibile risulta il sistema di riconoscimento basato sulla geometria delle vene, in cui vengono impiegate una telecamera e una luce a raggi infrarossi per catturare la struttura visibile dei vasi sanguigni presenti nella parte posteriore della mano o delle dita dell'individuo. Generalmente, si utilizza un algoritmo in grado di registrare automaticamente le caratteristiche della struttura vascolare[246]. La struttura dei vasi sanguigni rispetta il parametro di *univocità* e risulta abbastanza stabile nel corso della vita dell'individuo.

Le impronte palmari, invece, avendo caratteristiche (cd. "linee" e "rientranze") simili a quelle che si possono trovare nelle impronte digitali, presentano uno spiccato grado di *riferibilità individualizzante*[247]. A seconda della risoluzione del sensore[248], le immagini catturate possono contenere le principali venature, rughe oppure la risoluzione intera della geometria della mano.

---

[242] Con riferimento alla non univocità dell'impronta palmare, cfr. E. Yoruk, E. Kokukoglu, B. Sankur, *Shape-Based Hand recognition*, in *IEEE Transaction on Image Processing*, vol. 15, no. 7, 2006, pp. 1083-1815. In linea con tale posizione v. N. Balossino, S. Siracusa, *L'identificazione basata sul volto: metodi fisionomici e metrici*, in AA.VV., *Security Forum 2004*, ItaSForum, Milano, 2004, pp. 171-188: «occorre tener presente che la geometria può variare a causa dell'età e di fattori patologici, come per esempio l'artrite, e che inoltre non possiede elevata singolarità; ne segue che questo metodo, è accettabile (a parte fattori igienici per il posizionamento di tutta la mano sulla piastra di cattura), richiede facili metodologie di acquisizione riproducibili, non lede la privacy, ma viene tuttavia utilizzato solo quando vi siano minime esigenze di identificazione». Opinioni conformi sono anche quelle di A. Bera, D. Bhattacharjee, M. Nasipuri, *Hand Biometrics in Digital Forensics*, in AA.VV., *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications*, (a cura di) A.K. Muda et al., cit. e E. Belfatto, *La biometria applicata alla sicurezza e al contesto forense*, FDE Institute Press, Mantova, 2015, p. 96.
Salvo alcune iniziali pronunce (Cass. pen., Sez. II, 19.11.1975, n. 3999 in *CED Cass* n. 132938), di contrario avviso risulta, invece, la giurisprudenza della Corte di cassazione che ha di fatto equiparato in termini di univocità e immutabilità le impronte palmari a quelle digitali, confermandone, da tempi ormai risalenti, la piena validità probatoria [Cass. pen., Sez. II, 9.5.1985 n. 11220 in *CED Cass* n. 171197; Cass. pen., Sez. I, 20.5.1982 n. 7434 in *CED Cass* n. 154795; Cass. pen., Sez. I, 9.10.1981 n. 1253 in *CED Cass* n. 152085].

[243] Cfr. S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, cit., p. 31.

[244] Per es. per l'età o malattie.

[245] Il riconoscimento basato sull'impronta palmare, dal momento che richiede un necessario contatto fisico fra il sensore e la mano dell'individuo, è ritenuto particolarmente *invasivo*. Sul punto v. E. Yoruk, E. Kokukoglu, B. Sankur, *Shape-Based Hand recognition*, cit., pp. 1083 e ss.

[246] Si tratta dei vasi del sangue e i punti di ramificazione.

[247] Cfr. S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, cit., p. 31, in cui si sottolinea che le impronte palmari «possono essere suscettibili degli stessi problemi di durata e di danneggiamento dei sistemi biometrici basati sulle impronte digitali anche se dal momento che un palmo ha un'area di estensione più ampia, le sue caratteristiche hanno un carattere identificativo maggiore rispetto alle impronte digitali».

[248] Può essere ottico, a ultrasuono o termico.

Durante la fase di *enrollment*, al pari dei sistemi di riconoscimento delle impronte digitali, sono estratte le minuzie e/o caratteristiche palmari utilizzate, al fine di creare la rappresentazione digitalizzata del dato[249]. Quest'ultima può essere rappresentativa dell'intera superficie del palmo della mano o essere limitata ad alcune superfici specifiche[250]. Analogamente con quanto accade per le impronte digitali (cfr. il § 3.1.), posto che le condizioni di acquisizione dei campioni possono variare anche in modo rilevante[251], è sempre previsto che, in seguito alla comparazione automatica delle impronte, un operatore esperto verifichi attraverso un'analisi manuale il livello di compatibilità effettivo fra le stesse. Anche in questo caso, infatti, l'attribuzione definitiva dell'impronta viene eseguita da un operatore specializzato e non dalla macchina[252].

3.3. Il riconoscimento del volto[253]*

Fra i diversi accertamenti esteriori che è possibile compiere sulla persona, il volto ha assunto negli ultimi anni un ruolo di estremo rilievo[254]. I sistemi di riconoscimento facciale, rispetto ad altri metodi di riconoscimento biometrici[255], presentano un alto grado di *accettabilità*, dal momento che essi richiedono poca, o quasi nessuna, collaborazione da parte del soggetto passivo. Oltre a ciò, il sistema non risulta nemmeno assoggettabile a cambiamenti comportamentali, volontari o meno, da parte dell'individuo sottoposto al riconoscimento[256].

---

[249] L'attività di acquisizione del campione rientra ragionevolmente fra le attività di p.g. consentite ai sensi dell'art. 354 c.p.p. e 349 c.p.p.

[250] Il procedimento di confronto può basarsi sulle minuzie, sulle correlazioni o sulle venature.

[251] Cfr. K. Mather, *Elementi di biometria*, cit., p. 25.

[252] Cfr. A. Amato, G. Flora, C. Valbonesi, *Scienza, diritto e processo penale nell'era del rischio*, cit., p. 293.

[253]*Parte del presente paragrafo è costituito dai contributi E. Sacchetto, *Face to face*: *il complesso rapporto tra automated facial recognition technology e processo penale*, in *www.lalegislazionepenale.it*, 16.10.2020; E. Sacchetto, *Brevi riflessioni sui fondamenti e sui limiti del rapporto fra automated faced-based human recognition technology e processo penale*, in *ASTRID*, 2022 (in via di pubblicazione) e E. Sacchetto, *Automated faced-based human recognition technologies e procedimento penale alla luce della proposta di regolamento sull'IA: alcuni spunti di riflessione*, in AA.VV., *Collana del Centro Studi Giuridici del Dipartimento di Economia di Ca' Foscari*, (a cura di) C. Camardi, *atti del Convegno* "*La via europea per l'intelligenza artificiale*", Venezia il 25-26.11.2022 (in via di pubblicazione). In questa sede s'intende fornire solo brevi cenni sulle tecniche di base per il riconoscimento del volto che sarà oggetto di un più ampio approfondimento nel capitolo IV.

[254] Per un primo approfondimento sul tema cfr. G. Iovane, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza*, cit., p. 213, T. Alesci, *Il corpo umano come fonte di prova*, cit., pp. 89 e ss., G. Gulotta, E. M. Tuosto, *Il volto nell'investigazione e nel processo. Nuova fisiognomica Forense*, Giuffrè, Milano, 2017, pp. 114 e ss., J. Zheng, V. M. Patel, R. Chellapa, *Recent developments in Video-based Face recognition*, in AA.VV., *Handbook of biometrics for forensic science*, (a cura di) M. Tistarelli, C. Champod, Springer, Cham 2017, p. 149, N. Balossino, S. Siracusa, *L'identificazione basata sul volto: metodi fisionomici e metrici*, in https://docplayer.it/18656857-L-identificazione-basata-sul-volto-metodi-fisionomici-e-metrici.html, G. Preite, *Il riconoscimento biometrico. Sicurezza versus Privacy*, UNIService, Trento 2007, pp. 37 e ss., F. Cascetta, M. De Luccia, *Sistemi di identificazione personale*, in *Il Mondo Digitale*, n. 1, 2004, p. 49, S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, cit., p. 33.

[255] Cfr. L. Greco, A. Mantelero, *Industria 4.0, robotica e privacy-by-design*, in *Diritto dell'Informazione e dell'Informatica* (Il), fasc.6, 1.12.2018, p. 875.

[256] «*Personal identification systems based on faces have the advantage that facial images can be obtained from a distance without requiring cooperation of the subject, as compared to other biometrics such as fingerprint, iris, etc*». J. Zheng, V. M. Patel, R.

Nell'ultimo decennio, il procedimento di identificazione ha tratto evidenti vantaggi dall'impiego di dispositivi informatici: questi, infatti, consentono di estrarre caratteristiche fisionomiche non direttamente visibili e rendono agevoli confronti e valutazioni metriche[257]. D'altra parte, sempre più di frequente, fatti di cronaca hanno mostrato come tramite telecamere di videosorveglianza sia possibile risalire agevolmente all'autore del reato o all'identificazione della vittima[258], attraverso l'estrapolazione dell'immagine del volto di una persona[259]. Privati cittadini, aziende e amministrazioni pubbliche hanno cominciato a sviluppare la tendenza a disseminare impianti di videosorveglianza per scopi di tutela e prevenzione[260]: ne è conseguita la potenziale «acquisizione di una moltitudine di fotogrammi, con i quali è possibile riconoscere eventuali fatti di reato»[261]. In tali termini, l'atto di identificare un soggetto ignoto consiste nel comparare delle immagini estrapolate dai sistemi di videosorveglianza con quelle acquisite precedentemente e inserite in un archivio: la qualità del fotogramma influisce notevolmente sull'intero procedimento[262]. Se, per esempio, le riprese sono adeguatamente luminose e ricche di dettagli, saranno per lo più sufficienti confronti fisionomici. Lo

---

Chellapa, *Recent developments in Video-based Face recognition*, cit., p. 149. Cfr. anche A. Kumar, N. Kaur, Face Recognition, in *International Journal of Advanced Trends in Computer Applications (IJATCA)*, vol. 3, no. 2, 2016, pp. 10-15.

[257] Cfr. T. Alesci, *Il corpo umano fonte di prova,* cit., p. 90.

[258] A titolo esemplificativo, v. https://www.ilgiorno.it/milano/cronaca/stupratori-1.5885658 ; https://www.ilgiorno.it/milano/cronaca/ragazzina-ritrovata-1.5466752 e https://questure.poliziadistato.it/it/Frosinone/articolo/24815fe9d21c8b40b462215968.

[259] Cfr. T. Alesci, *Il corpo umano fonte di prova,* cit., p. 90.

[260] La l. 23.4.2009 n. 38, in materia di sicurezza pubblica, ha permesso ai Comuni la possibilità di installare videocamere per la tutela della "sicurezza urbana" negli spazi pubblici. V. https://www.camera.it/parlam/leggi/09038l.htm. Oltre a ciò, vi sono diversi Comuni italiani che hanno richiesto di inserire le telecamere dei privati nella rete di sorveglianza a disposizione delle forze dell'ordine, come avviene per esempio a Milano con l'Anagrafe Telecamere oppure a Piacenza: lo scopo sarebbe quello di "mappare" la posizione delle telecamere private che riprendono aree esterne aperte al pubblico. V. https://www.comune.milano.it/aree-tematiche/polizia-locale-e-sicurezza/progetti/anagrafe-telecamere e http://www.anagrafetelecamere.it/ (visualizzato in data 20.1.2021).

[261] «L'obiettivo è quello di consentire il cd "riconoscimento facciale tra la folla". Il sistema del "*Biometric Optical Surveillance System*" (Boss), secondo un recente studio del *New York Times* consentirebbe di scansionare intere folle ed identificare presunti terroristi. Il riconoscimento facciale avviene attraverso macchine dotate di sensori ad infrarossi che fotografano diverse angolature del volto. I dati così raccolti, vengono poi elaborati da un software, al fine di verificare la corrispondenza con il volto di presunti terroristi catalogati nel *database*». T. Alesci, *Il corpo umano fonte di prova,* cit., p. 89.

[262] Il volto può essere interessato da processi di invecchiamento, diverse espressioni facciali, variazioni di illuminazione e dello sfondo dell'ambiente circostante, da variazioni di posizioni rispetto alla telecamera, dalla presenza di occhiali etc. Cfr. M. Singh, S. Nagpal, R. Singh, M. Vatsa, *On Recognizing face images with weight and age variations*, in *Proc. IEEE Digital Object Identifier*, vol. 2, 2014, G. Guo, G. Mu, and K. Ricanek, *Cross-age face recognition on a very large database: the performance versus age intervals and improvement using soft biometric traits*, in *Proc. 20th Int. Conf. Pattern Recognit*., 2010, pp. 3392-3395, U. Park, Y. Tong, A. K. Jain, *Age-invariant face recognition*, in *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 5, pp. 947954, 2010. E, ancora, «(…) *automated face recognition actually subsumes a number of separate problems. In identity verification, the subject looks straight at the camera under controlled lighting conditions, and their face is compared with the one on file. A related but harder problem is found in forensics, where we may be trying to establish whether a suspect's face fits a low-quality recording on a security video*» Y. Adini, Y. Moses, S. Ullman, *Face recognition: The Problem of Compensating for Changes in Illumination Direction*, in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, v. 19, no. 7, 1997, pp. 721–732. Al fine di risolvere tali problematiche, sono state avanzate diverse soluzioni, tra cui si v. il progetto di R. R. Devaram, A. Ortis, S. Battiato, A. R. Bruna, V. Tomaselli, *Real-Time Thermal Face Identication System for Low Memory Vision Applications Using CNN*, in *Pattern Recognition. ICPR International Workshops and Challenges*, Springer Professional, 2021.

studio delle caratteristiche del volto richiede, infatti, l'individuazione di particolari siti anatomici, detti *punti di repere*[263], utili sia per la rappresentazione di strutture morfologiche sia per la valutazione dei diversi aspetti somatici.

A seguito dell'evoluzione tecnologica, il sistema biometrico basato sul riconoscimento del viso è divenuto un procedimento automatico o semi-automatico che compara e pone in luce le differenze della struttura geometrica del volto[264], tra cui la configurazione dei suoi attributi e le loro relazioni geometriche, compiendo un'analisi metrica dell'immagine e del tessuto della pelle[265].

Se il procedimento è attivato per sorvegliare dal vivo l'accesso a particolari strutture, il riconoscimento dei volti (*face recognition*) richiede che un sistema informatizzato analizzi in pochi attimi i dati a disposizione e ne ricavi una sorta di "cartografia facciale" che viene confrontata con quelle registrate in precedenza negli archivi degli organi di sorveglianza. Il riconoscimento avviene nella maggior parte dei casi sulla base di tecniche neurali che simulano il processo di apprendimento umano[266].

Quando invece si deve procedere all'identificazione in un tempo differito, come per esempio nel caso in cui si debba comparare l'immagine di un soggetto ripreso da telecamere di videosorveglianza nell'atto di compiere un reato a quella di un insieme di indagati, il metodo adottato richiede sempre una valutazione fisionomica e metrica da parte di un operatore esperto, per giungere a un giudizio di identificazione o esclusione, spendibile come prova nel giudizio. In tal senso, come si approfondirà meglio *infra* nei capitoli III e IV, i software automatici di riconoscimento sono ad oggi utilizzati solo

---

[263] «I principali punti di *repere* sono: il *nasion* (radice del naso); *glabella* (punto situato al di sopra della radice del naso, dove la cute è in genere priva di peluria); *pronasale* (punto più sporgente della punta del naso); *naso spinale* (punto corrispondente al sottosetto nasale); *alare* (punto più sporgente dell'ala del naso); *prosthion* (punto superiore del solco naso labiale); *gonion* (margine inferiore del ramo della mandibola); *gnathion* (sporgenza inferiore del mento); *trichion* (punto di attacco dei capelli sulla fronte); *vertex* (punto più alto del cranio); *zygion* (punto più sporgente dello zigomo)». N. Balossino, S. Siracusa, *L'identificazione basata sul volto: metodi fisionomici e metrici*, Security Forum, Edizioni ItasForum, Bergamo, 2004, p. 4.

[264] Gli occhi, le sopracciglia, le labbra e il mento.

[265] Durante la rilevazione dei dati, un sensore (ad esempio una telecamera) cattura un'immagine o una serie di immagini del volto del soggetto che vengono convertite in formato digitale. A questo punto è possibile procedere alla sua memorizzazione, per esempio, su una *smart card* o su un passaporto, utili per i procedimenti di verifica dell'identità. Per un approfondimento sulla differenza fra software valutativi e non valutativi, si veda S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 100.

[266] Sebbene s'intenda approfondire l'ambito delle tecniche di intelligenza artificiale applicate ai software di riconoscimento biometrico nel successivo capitolo II, giova qui evidenziare che: «i sistemi automatici che operano per mezzo di software progettati sul modello delle reti neuronali del cervello umano, non pensano, ovviamente, in via autonoma, ma "pensano" imitando il pensiero dell'uomo, il che è reso possibile dalla lettura e successiva elaborazione dei *big data*, utilizzati, ad esempio, per decifrare immagini diagnostiche oppure per riconoscere una voce o un volto» R. Lopez, *Riconoscimento facciale tramite software e individuazione del sospettato*, in AA.VV, *Pre-investigazioni (espedienti e mezzi)*, (a cura di) A. Scalfati, Giappichelli, Torino, 2020, p. 296. «*A neural network is a computing framework which consists of massively parallel interconnection of flexible neural processors and because of its parallel quality it can execute computations at a very high rate as compared with the previous techniques and because of its adaptive nature, it can acclimate to variations in the data and learn the attributes of the inputted signal. The output is fed from one node to another one in the network and the final decision is made which depends on the interaction of all nodes. There are various approaches available for training of neural networks*». A. Kumar, N. Kaur, Face Recognition, in *International Journal of Advanced Trends in Computer Applications (IJATCA)*, vol. 3, 2, 2016, p. 12.

come supporto iniziale e meramente "orientativo" per l'attività investigativa. Maggiore importanza riveste l'operazione di confronto fisionomico successiva, compiuta da un operatore esperto, il quale una volta eseguita l'analisi morfologica delle singole caratteristiche facciali[267], si esprimerà in termini di "livelli" di compatibilità fra i due volti. L'operazione di comparazione e analisi morfologica compiuta dall'esperto, se eseguita durante la fase delle indagini preliminari, rientrerebbe tra gli accertamenti tecnici ripetibili *ex* art. 354 c.p.p. che non necessitano della presenza obbligatoria del difensore per il conferimento dell'incarico e durante l'espletamento dello stesso.

3.3.1. Cenni sul sistema A.F.I.S. – S.S.A.

Fino alla metà degli anni '80 e più diffusamente agli albori degli anni '90, l'impiego delle impronte digitali nelle indagini penali è stato condizionato dall'assenza di sistemi operativi per un confronto immediato, automatico e a largo raggio, come quello attuabile grazie all'A.F.I.S. ("*Automated Fingerprint Identification System*")[268]. L'A.F.I.S. è una banca dati informatica per la raccolta e la comparazione delle impronte digitali[269]. Il sistema, acquisita per azione di un operatore un'impronta digitale o un frammento di essa da confrontare, propone una lista di possibili candidati che decresce proporzionalmente al grado di similarità fra i dati confrontati. A questo punto, il risultato pseudonimizzato viene completato con i dati della persona ed è trasmesso all'unità di polizia giudiziaria richiedente. Infatti, A.F.I.S. è strutturato in modo tale che l'insieme delle impronte digitali siano fisicamente separate rispetto alle informazioni afferenti alle persone. Solo nel caso in cui il

[267] «*Any standard procedure using facial comparison analysis should consider all of the following facial components: skin, face/head outline, face/head composition, hair, forehead, eyebrows, eyes, cheeks, nose, ears, mouth, chin/jawline, neck, facial hair, facial lines, scars, facial marks, and alterations*». FISWG, *Facial Comparison Overview and Methodology Guidelines*, disponibili su https://fiswg.org/documents.html (ultima visualizzazione in data 23.2.2021).

[268] Da ora in avanti A.F.I.S. Cfr. P. Komarinski, *Automated fingerprint identification systems* (AFIS), Elsevier Academic, Amsterdam, 2005 e L. Scaffardi, *Dati genetici e biometrici: nuove frontiere per le attività investigative*, in AA.VV., *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale,* (a cura di) L. Scaffardi, Giappichelli, Torino, 2018, pp. 37-64. La banca dati è usufruibile dalla Polizia di Stato, per i 14 Gabinetti Regionali di Polizia Scientifica situati a Milano, Torino, Padova, Genova, Bologna, Cagliari, Firenze, Ancona, Roma, Napoli, Bari, Reggio Calabria, Palermo e Catania. Per l'Arma dei Carabinieri, il sistema è utilizzato da i RIS di Roma, Parma, Cagliari e Messina. Tramite un servizio centralizzato, l'Arma dei Carabinieri rende disponibile a tutti i Comandi dotati di apparato foto segnalatore (Nuclei Operativi di Comando Compagnia - Reparti Operativi di Comando Provinciale) la possibilità di effettuare comparazioni A.F.I.S. A tali strutture accedono tutti gli altri Reparti dell'Arma dei Carabinieri, fino a quelli di minore livello ordinativo. Per un approfondimento v. http://www.profilecrime.it/IMPRONTE1.htm (visualizzato in data 20.11.2020).

[269] All'A.F.I.S. si affianca l'A.P.I.S. ("*automated palmprint identification system*"), banca dati di impronte palmari che viene utilizzata generalmente quando le impronte digitali risultano abrase o illeggibili. Come osservato da A. Spinella, G. Solla, *L'identificazione personale nell'investigazione scientifica: Dna e impronte*, in *Cass. pen*., fasc. 1, vol. 49, 2009, p. 433, l'A.F.I.S. rappresenta: «una banca dati informatica per la raccolta e la comparazione delle impronte digitali. Il sistema, acquisita per azione dell'operatore un'impronta digitale o un frammento di essa da confrontare, propone una lista di possibili candidati che decresce proporzionalmente alla verosimiglianza. (…) L'A.F.I.S. è oggi il più consistente archivio di dati personali a disposizione delle forze dell'ordine di polizia: contiene i cartellini segnaletici, comprensivi di dati fotografici e biometrici, di circa quattro milioni di persone, per un totale comprensivo di circa sessanta milioni di impronte immagazzinate».

lancio di una ricerca produca effettivamente una corrispondenza con un'impronta registrata, è possibile risalire alle informazioni complete sulla persona.

Giova ricordare che il risultato di compatibilità tra due impronte digitali, restituito dal software collegato alla banca dati A.F.I.S., consiste unicamente in un giudizio di similarità fra i due dati, espresso in forma percentuale. Infatti, la banca dati contiene un numero limitato di impronte digitali, che, seppure sia molto elevato, non corrisponde all'intera popolazione. Questo significa che, una volta che il software abbia misurato un dato livello di compatibilità fra due impronte, espresso come giudizio di similarità fra le stesse, occorre l'ulteriore calcolo del cd. "rapporto di verosiglianza" al fine di valutare se la traccia di un'impronta digitale e un campione di riferimento provengano effettivamente da fonti comuni o diverse[270].

Ad oggi, A.F.I.S. rappresenta il più consistente archivio di dati personali a disposizione delle forze di polizia: contiene i cartellini segnaletici, comprensivi di dati fotografici e biometrici, di circa quattro milioni di persone, per un totale di circa sessanta milioni di impronte immagazzinate[271]. L'impiego di A.F.I.S. è sostanzialmente duplice: la ricerca decadattilare preventiva e l'analisi di un frammento papillare in ambito giudiziario. Nel primo caso, l'indagine ha ad oggetto i cartellini segnaletici prodotti dalle forze di polizia a carico di un soggetto arrestato o fermato per motivi di pubblica sicurezza[272]. Nel secondo, invece, la ricerca nella banca dati costituisce una fase del procedimento di identificazione della persona nei cui confronti vengono svolte le indagini.

Con riferimento al sottosistema anagrafico S.S.A., invece, s'intende l'applicativo attualmente utilizzato dagli operatori di Polizia Scientifica per la gestione e la ricerca dell'identità di un soggetto sconosciuto all'interno della banca dati dei soggetti fotosegnalati[273]. Tale estensione S.S.A. si

---

[270] Su questo punto v. D. Meuwly, D. Ramos, R. Haraksim, *A guideline for the validation of likelihood ratio methods used for forensic evidence evaluation*, in *Forensic Science International*, vol. 276, 2017, pp. 142-153 e D. Ramos, R. Haraksim, D. Meuwly, *Likelihood ratio data to report the validation of a forensic fingerprint evaluation method*, in *Data in Brief*, vol. 10, 2017, pp. 75-92.

[271] A.F.I.S. costituisce un fondamentale strumento anche nell'ottica dello scambio di informazioni tra gli organi investigativi dei diversi Stati; sotto questo aspetto va anticipato che la decisione 2008/615/GAI prevede l'accesso reciproco degli Stati membri ai sistemi automatizzati di identificazione dattiloscopica. Cfr. il capitolo II, § 1.5.1.2.

[272] Una volta scansionato il cartellino segnaletico, esso viene inviato al Gabinetto di Polizia Scientifica ovvero al Reparto Dattiloscopia Preventiva dei Carabinieri. A questo punto, il dattiloscopista procede al controllo sulla qualità delle impronte eseguendo successivamente una ricerca nel database, il quale, in pochi minuti propone una serie di candidati compatibili, concludendo così l'accertamento tecnico, con un responso che può essere negativo o positivo. Il risultato negativo dell'accertamento implica che il soggetto sottoposto ai rilievi non è stato fotosegnalato in precedenza, l'esito positivo, invece, mostra come lo stesso sia stato fotosegnalato altre volte, indicando contestualmente i dati d'interesse (per es. la data dei rilievi, il reparto segnalante e il motivo del fotosegnalamento).

[273] Decreto del Ministero dell'Interno 24.5.2017, relativo alla «individuazione dei trattamenti dei dati personali effettuati dal Centro elaborazione dati del Dipartimento di pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, in attuazione dell'art. 53, comma 3, d.lgs. 30 giugno 2003, n. 196», in G.U., Suppl. ord., n. 145, 24.6.2017.

interfaccia con la banca dati A.F.I.S., tramite un apposito software *batch*[274], a cui "si allinea" recuperando da essa i nuovi inserimenti[275]. La banca dati A.F.I.S., dunque, grazie all'ulteriore estensione dell'applicativo S.S.A., permette agli organi di polizia di eseguire ricerche basate sia su campioni di impronte digitali, sia sui volti dei soggetti indagati[276]. Il funzionamento della comparazione è lo stesso: prima il software restituisce il risultato di compatibilità o meno fra due volti, espresso in termini di giudizio di similarità; successivamente occorre che un esperto verifichi quel dato calcolando il "rapporto di verosimiglianza" rispetto ad una data popolazione di riferimento[277].

3.4. La misurazione dell'iride e della retina

Un'ulteriore tecnica di riconoscimento si basa sull'iride, la porzione colorata dell'occhio che circonda la pupilla scura, racchiusa nei tessuti bianchi del bulbo oculare (cd. *sclera*). Essa è costituita da fibre muscolari per mezzo delle quali la pupilla viene dilatata al fine di regolare la quantità di luce che entra nell'occhio. Sia la disposizione delle fibre muscolari che le pigmentazioni rendono il tratto

---

Ogni dato registrato nella banca dati si compone di ulteriori informazioni, tra cui un'immagine fotosegnaletica memorizzata su un meccanismo con il quale i file sono posizionati e organizzati su dispositivi informatici utilizzati per l'archiviazione dei dati, cd. *filesystem*, e un insieme di dati strutturati anagrafici e/o descrittivi memorizzati all'interno di un database. Le immagini fotosegnaletiche si trovano in formato jpeg e di qualità e composizione eterogenea dipendente dal tipo di dispositivo di acquisizione, dal motivo del fotosegnalamento e dal periodo storico in cui tale immagine è stata inserita nella banca dati. Posto che un soggetto può essere sottoposto a fotosegnalamento più volte, potrà verificarsi l'eventualità che differenti *record* siano legati da un unico Codice Univoco Identificativo (CUI). S.S.A. permette la ricerca dei soggetti sottoposti a fotosegnalamento sulla base dei campi anagrafici e descrittivi associati alle immagini. L'amministrazione risulta essere proprietaria della documentazione e del codice sorgente sia dell'applicativo S.S.A. sia del *batch* di allineamento dei dati tra A.F.I.S. ed S.S.A. Cfr. MINISTERO DELL'INTERNO DIPARTIMENTO DELLA PUBBLICA SICUREZZA, *Capitolato tecnico. Procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini S.A.R.I.*, reperibile all'indirizzo https://www.poliziadistato.it/statics/06/20160627-ct-sari--4-.pdf (visualizzato in data 20.12.2021).

[274] Cfr. P. B. Hansen, *Classic Operating Systems: From Batch Processing to Distributed Systems*, Springer, New York, 2001.

[275] Così, la scheda tecnica n. 19 del Decreto del Ministero dell'Interno 24.5.2017, ha specificato come A.F.I.S. operativo presso il servizio di polizia scientifica della Direzione centrale Anticrimine della Polizia di Stato, gestisca il trattamento dei dati personali e identificativi acquisiti dai soggetti sottoposti a foto segnalamento a fini, tra gli altri, di: identificazione dattiloscopica di soggetti foto segnalati (art. 349 c.p.p.; art. 4 T.U.L.P.S. e art. 7 Regolamento di esecuzione; art. 5, d.lgs. n. 286/1998; legge n. 85/2009; Regolamento UE n. 603/2013; Provvedimento generale prescrittivo in tema di biometria del Garante per la protezione dei dati personali n. 513/2014); esecuzione di accertamenti tecnici volti alla identificazione dei frammenti di impronta acquisiti sulla scena del crimine o sui reperti pertinenti al reato, in relazione a indagini condotte attraverso accertamenti tecnici effettuati dalle Forze di polizia nell'ambito di un procedimento penale (Titolo IV e V c.p.p.; Provvedimento generale prescrittivo in tema di biometria del Garante per la protezione dei dati personali n. 513/2014); accertamenti per finalità investigativa mediante il sottosistema anagrafico (Titolo IV e V c.p.p.; art. 13 l. n. 124/2007; Provvedimento generale prescrittivo in tema di biometria del Garante per la protezione dei dati personali, n. 513/2014).

[276] Le funzionalità delle due banche dati in questione sono state implementate all'interno del software S.A.R.I. *Enterprise* (cfr. *infra* il capitolo IV), con l'obiettivo di garantire una soluzione applicativa unica, in grado di articolare la ricerca su un triplice livello: sulla base del volto, avendo a disposizione un'immagine anche estrapolata da un file proveniente dalla video-sorveglianza, su base anagrafica/descrittiva, tenendo, dunque, in considerazione le informazioni anagrafiche o descrittive associate alle immagini nella banca dati dei foto segnalati e infine, su base combinata, elaborata tramite integrazione di entrambe le tipologie di dati. R. Lopez, *Riconoscimento facciale tramite software e individuazione del sospettato*, cit., p. 300.

[277] Su questo punto si tornerà meglio *infra* al capitolo IV.

in esame altamente *distintivo*[278]. Tale sistema richiede uno specifico apparato di cattura dell'immagine dell'occhio[279], nonché l'uso di appropriati software che isolano e trasformano la sezione dell'iride in modelli, denominati "sagome"[280].

I limiti principali di tali tecniche di riconoscimento sono essenzialmente legati al fatto che questi necessitano di uno specifico posizionamento dell'utente, e alla circostanza che il dato biometrico sia soggetto a mutamento nel corso della vita dell'individuo[281]. Oltre a ciò, le tecniche di rilevamento dei dati sono considerate altamente *invasive* e vi sono ancora alcune perplessità circa i rischi di danneggiamento agli occhi[282]. Per tale ragione, questi sistemi di riconoscimento non sono, al momento, impiegati in ambito giudiziario.

Gli strumenti automatizzati basati sulla retina si fondano invece sul raffronto della complessa struttura dei vasi sanguigni che si trovano nella parte posteriore dell'occhio. In particolare, una luce a raggi infrarossi illumina i vasi che si trovano dietro la retina e li riflette con diverse lunghezze d'onda. Il sistema di vascolarizzazione della retina costituisce un parametro *universale* e di elevata *affidabilità*, ma una volta rilevato è difficile da collezionare e lo strumento è considerato generalmente *invasivo*[283].

Entrambi i sistemi di riconoscimento risultano ad oggi per lo più sfruttati in ambito autenticativo (1:1). Come poc'anzi accennato, più dubbio è l'impiego per finalità identificative in contesti giudiziari, ad oggi ancora mai avvenuto, nemmeno a fini di mero orientamento delle indagini.

---

[278] «*The iris is fully formed by the eight month of gestation and remains (partially) the same throughout one's lifetime*», S. Smyth, *Biometrics, surveillance and the law*, cit., pp. 25 e ss.

[279] Il soggetto guarda verso il sensore e la struttura della sua iride viene illuminata da un laser a bassa intensità. Un flusso di luce infrarossa, a questo punto, effettua la scansione dell'occhio e consente di rilevare le sue peculiarità.

[280] In particolare, la scansione dell'iride avviene mediante una video-camera ad una distanza di circa 40 centimetri e non richiede alcun contatto con il sensore. Nonostante le dimensioni dell'iride varino in funzione dell'illuminazione ambientale (una forte luce fa restringere la pupilla e di conseguenza aumentare il raggio della corona dell'iride), un apposito algoritmo tiene conto di queste modifiche e della eventuale copertura superiore ed inferiore dell'iride dovuta alle palpebre. La dimensione del modello è approssimativamente di 500 *bytes* (Cfr. GRUPPO DI STUDIO PER LA DEFINIZIONE DI INIZIATIVE NEL CAMPO DELLA BIOMETRIA, *Brevi note sulle tecnologie biometriche in un contesto ICT*, in https://www.privacy.it/archivio/cnipabiometria.html - ultimo accesso in data 15.01.2021). In ragione della specifica e costosa apparecchiatura della quale necessita tale sistema di riconoscimento, le applicazioni risultano ancora ristrette a poche aree. Infatti, i settori di applicazione di tale tecnica riguardano essenzialmente l'accesso fisico ad un determinato luogo o a zone riservate e in ambito di alta sicurezza (cfr. https://www.aeroporto.net/aeroporto-amsterdam/terminal-aeroporto-amsterdam/ - ultimo accesso in data 15.01.2021).

[281] Malattie dell'occhio, come per es. il glaucoma, oppure interventi chirurgici specifici tendono ad alterare la struttura dell'iride. S. Amato, F. Cristofari, S. Raciti, *Biometria*., cit., p. 35.

[282] Cfr. S. Amato, F. Cristofari, S. Raciti, *Biometria*., cit., p. 35.

[283] Cfr. S. Amato, F. Cristofari, S. Raciti, *Biometria*., cit., p. 35.

3.5. Il riconoscimento basato su aspetti dinamici

3.5.1. Il riconoscimento vocale: lo stato dell'arte

Negli ultimi anni, si è registrato un ricorso sempre più frequente alle investigazioni vocali, progressivamente amplificato anche a causa della rilevante diffusione di dispositivi per la comunicazione a distanza e delle diverse forme di comunicazione via internet[284]. Per tale ragione, l'impronta fonica, più di altri tratti, è stata oggetto di numerosi studi di cui tuttavia non si ritiene possibile dar conto in modo esaustivo in questa sede. Pare in ogni caso doveroso porre in luce alcuni snodi fondamentali della materia, analogamente a quanto riportato per altre tecniche di identificazione.

I sistemi biometrici basati sul riconoscimento vocale si fondano sulla misurazione della voce, componente comportamentale dell'individuo risultante dai suoi tratti fisici[285], posto che le caratteristiche della voce derivano dalla forma e dalla grandezza dei tratti vocali, dal mento, dalle cavità nasali e dalle labbra[286]. La voce, pur avendo delle caratteristiche proprie riconoscibili, è soggetta a una forte *variabilità* (cfr. il § 1.1). L'anatomia dell'individuo (lunghezza delle corde vocali e, più in generale, conformazione dell'apparato fonatorio) definisce solo i limiti - in termini di "alti e bassi" - del timbro vocale[287]. All'interno di questi, la voce si muove, condizionata da molteplici fattori: particolari stati patologici (un banale raffreddore o altre malattie, ma anche l'assunzione di droghe o alcool), condizioni emotive e di contesto[288]. Dal punto di vista del riconoscimento vocale, dunque, il

---

[284] Cfr. K. La Regina, *L'identificazione della voce nel processo penale*, Wolters Kluwer, Milano, 2018, R. Valli, *Le indagini scientifiche nel procedimento penale*, Giuffrè, Milano, 2013, pp. 749 e ss., S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, cit., pp. 37 e ss., P. Felicioni, *Il riconoscimento del parlante tra prassi e modelli normativi*, in AA.VV., *Le indagini atipiche*, (a cura di) A. Scalfati, Giappichelli, Torino, 2019, pp. 259 e ss., C. Ciampini, *Indagini foniche*, in AA.VV., *Scienze forensi. Teoria e prassi dell'investigazione scientifica*, (a cura di) M. Picozzi, A. Intini, Utet, Torino, 2009, p. 405.

[285] Sul punto, A. Contaldo, *Biometrie e documenti di viaggio*, in *L'amm. it*., 2007, p. 213 e A. Paoloni, *Le indagini foniche*, in http://www.ording.roma.it/archivio/file/articolo_odi_v_4.pdf; di altro avviso è il GRUPPO PER LA TUTELA DEI DATI PERSONALI (organo consultivo e indipendente dell'Unione Europea in tema di tutela dei dati e della vita privata, istituito ai sensi dell'art. 29 della direttiva 1995/46/CE), *Documento di lavoro sulla biometria*, 2003, consultabile sul sito http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1609419, ove si ritiene che la voce rientri nella categoria dei parametri fisiologici; altri ancora (G. Preite, voce *Biometria*, in *Enciclopedia di bioetica e scienza giuridica*, vol. II, Edizioni Scientifiche Italiane, Napoli, 2009, p. 235) la collocano tra gli indicatori comportamentali. Non essendoci unanimità di vedute in dottrina, ne consegue che il riconoscimento vocale sia considerato dai più un metodo tecnicamente ibrido tra la biometria fisiologica e comportamentale poiché l'emissione è determinata non solo dalla conformazione anatomica della gola e della laringe, ma anche da aspetti comportamentali dell'utente come il tono umorale.

[286] La voce da un punto di vista fisico è un'onda acustica che si diffonde tramite un mezzo di propagazione come l'aria e si tratta di un risultato acustico di più fenomeni, a cominciare dal passaggio di aria attraverso la glottide. Cfr. F. Albano Leoni, P. Maturi, *Fonetica sperimentale e fonetica giudiziaria*, in *Giust. pen*., 1991, I, c. 316, G. Zambonini, *Metodi di riconoscimento della voce*, in AA.VV., *Le indagini scientifiche nel procedimento penale*, (a cura di) R.V.O. Valli, Milano, 2013, p. 750, S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, cit., pp. 37 e ss.

[287] Cfr. A. Paoloni, *La voce come elemento di identificazione della persona*, in AA.VV., *La voce come bene culturale*, (a cura di) A. De Dominicis, Roma, 2002, p. 129

[288] Cfr. F. Albano Leoni, P. Maturi, *Fonetica sperimentale e fonetica giudiziaria*, cit., p. 316, S. Chimichi, *Profili giuridici del riconoscimento del parlante*, in AA.VV., *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, (a cura di) C. Conti,

dato biometrico non è fisso, ma presenta un'«area di variabilità»[289], la quale, peraltro, può in parte coincidere con quella che connota qualcun altro. Ne consegue che il timbro vocale costituisce un bioindicatore dotato di una capacità "caratterizzante" imperfetta. Pertanto, l'identificazione sconta già un vizio di fondo, legato all'intrinseca incertezza che caratterizza l'oggetto dell'attività probatoria. Muovendo da tale premessa e volendo fornire una ricostruzione dello stato dell'arte in materia, si ritiene utile comprendere se, e in quale misura, tale incertezza si rifletta sulle diverse tecniche di riconoscimento e ne influenzi il funzionamento e la disciplina. Vi sono essenzialmente due modalità per attribuire l'identità a partire dalla voce. In primo luogo, l'ascolto basato sulla capacità dell'orecchio di stabilire la compatibilità fra differenti segnali vocali[290]. In secondo luogo, l'identificazione può essere effettuata attraverso dei software che confrontano due o più campioni (con un metodo di comparazione 1:1)[291], valutando il rapporto tra la probabilità che essi appartengano alla stessa persona e la probabilità che provengano da soggetti differenti. Vi sono sistemi automatici[292] e

Milano, 2011, p. 382-383, A. Paoloni, *La voce come elemento di identificazione*, cit., p. 126 afferma che «[una] parola o una frase ripetute nello stesso modo, dalla stessa persona, risultano comunque diverse tra loro, seppur di poco». Dello stesso avviso R. V. O. Valli, *Le indagini scientifiche nel procedimento penale*, cit., p. 749: «la cd. "impronta vocale", che caratterizza la voce di un essere umano e permette di dare un'identità alle voci anonime, presenta delle peculiarità del tutto diverse da quelle che si possono riscontrare in altri parametri biometrici, come le impronte digitali o l'impronta genetica. (…) la voce umana è una rappresentazione indiretta di un processo complesso che coinvolge non solo l'anatomia, ma anche la psicologia della persona che parla, e può cambiare in base alle inflessioni dialettali, al mezzo ovvero se scritta o parlata, alla situazione comunicativa se formale o informale, al ceto sociale, al sesso e all'età».

[289] T. Bove, P. E. Giua, A. Forte, C. Rossi, *Un metodo statistico per il riconoscimento del parlatore*, in *Statistica*, 2002, p. 475, efficacemente osservano: «se noi immaginiamo la molteplicità delle misure che caratterizzano un parlatore [...] in uno spazio multidimensionale, vediamo che non è un singolo punto che caratterizza un parlatore, ma un'area di variabilità».

[290] Il meccanismo ricognitivo si fonda sulla cd. memoria ecoica, ossia la capacità di ritenere informazioni apprese mediante il canale acustico. Cfr. G. Gulotta, *Psicologia della testimonianza*, in AA.VV., *Trattato di psicologia giudiziaria nel sistema penale*, (a cura di) G. Gulotta, vol. I, Giuffrè, Milano, 1987, p. 499. L'esistenza di "impronte foniche", cioè di caratteristiche individuali e irripetibili di una voce, analoghe alle impronte digitali, ha un suo importante fondamento proprio nella capacità soggettiva di riconoscere una persona ascoltandola parlare. Vedi F. Albano Leoni, P. Maturi, *Fonetica sperimentale e fonetica giudiziaria*, cit., p. 316.

[291] Cfr. *supra* il § 2.4. Peraltro s'intende qui dar conto del programma SIIP, *Speaker Identification Integrated Project*, un progetto finanziato dalla Commissione Europea che si prefigge di sviluppare un sistema per l'identificazione dei parlatori che, avvalendosi di un database in cui confluiscono chiamate intercettate, file audio-video e contenuti diffusi sui *social media* o su qualsiasi altro tipo di mezzo o canale di comunicazione, permetterà di superare il problema dell'utilizzo di identità nascoste o false da parte dei terroristi e dei criminali che utilizzano Internet per evitare di essere intercettati, identificati e monitorati. Per un approfondimento v. K. Khelif et al., *Towards a Breakthrough Speaker Identification Approach for Law Enforcement Agencies: SIIP*, in *2017 European Intelligence and Security Informatics Conference (EISIC)*, 2017, pp. 32-39. A livello nazionale, invece, l'Arma dei Carabinieri sta attualmente lavorando su un progetto per dotare alcuni nuclei investigativi presenti sul territorio di sistemi di riconoscimento 1:N, 1:N+1. Il risultato scaturente da questi software dovrà essere inviato al Reparto competente per territorio al fine di eseguire un confronto 1:1 e consentire di risalire alla voce ricercata. Il progetto prevede poi una seconda fase di condivisione dei dati attraverso la creazione di una banca dati centrale presso il Reparto di Roma nel quale convogliare e depositare tutte le impronte vocali. L'ultimo obiettivo prevede il coinvolgimento di altre forze di polizia per la creazione di una banca dati simile a quella del Dna (cfr. *infra* il § 3.6.3). Per un approfondimento cfr. K. La Regina, *L'identificazione della voce nel processo penale*, reperibile all'indirizzo https://www.letture.org/l-identificazione-della-voce-nel-processo-penale-katia-la-regina (visualizzato in data 25.6.2021).

[292] In questo caso, l'analisi risulta molto rapida ma imprecisa, poiché il calcolatore non è in grado di individuare gli spezzoni utili e prendere in considerazione ciascun segnale, anche esterno alla voce, come i rumori di fondo. Cfr. M. Nunziati, *Note sul*

semi-automatici[293], a seconda che l'algoritmo alla base del software proceda direttamente alla comparazione ovvero che vi sia un'iniziale fase di selezione del materiale da parte di un operatore esperto[294]. Inoltre, nell'ambito del riconoscimento vocale, si è soliti distinguere tra test "chiusi", in cui l'impronta fonica appartiene certamente a uno dei soggetti partecipanti all'esame, e test "aperti"[295], in cui la voce non appartiene a nessuno dei soggetti che vi prendono parte.

Ciascuna procedura è scandita in due fasi fondamentali: il *training* e il *test*. Il funzionamento del software, sia automatico sia semi automatico, si basa su una serie di operazioni funzionali che stimano la distribuzione della distanza del parlatore anonimo da se stesso (cd. variabilità intra-individuale) e quella della distanza dell'anonimo da tutti gli altri soggetti parlatori appartenenti alla stessa comunità linguistica inseriti in un database (cd. variabilità inter-individuale). Come accade per la generalità dei software di riconoscimento biometrico, viene definito un valore soglia che delimita il confine fra la variabilità della voce associata ad uno stesso soggetto e quella associata a soggetti diversi. Dopodiché, si procede con la comparazione fra la voce anonima e quella del "riconoscendo": se la distanza tra le due impronte foniche è inferiore al valore di soglia, sussiste una probabilità molto elevata che le voci appartengano ad un diverso soggetto e l'elaboratore esprimerà un giudizio di dissimilarità.

A questo punto occorre domandarsi quale sia l'approccio prevalente nella prassi giudiziaria in tema di riconoscimento del parlatore e quali siano le questioni più rilevanti dal punto di vista processuale[296].

Muovendo dal riconoscimento eseguito da un determinato soggetto, da tempo l'esperienza giudiziaria e gli studi di psicologia hanno posto in luce che la ricognizione basata sulla memoria, il ricordo e l'evocazione presenta un alto grado di fallibilità[297]. Accanto a variabili cd. "endogene", che partecipano all'atto della ricognizione da parte dell'individuo e che dipendono dalla capacità razionale

riconoscimento del parlante, in http://www.teutas.it/societa-informazione/prova-elettronica/381-note-sul-riconoscimento-del-parlante.html (ultimo accesso il 10.1.2021).

[293] Con riferimento ai metodi semi-automatici, invece, è possibile eseguire un'operazione di "filtraggio" attraverso la quale si è in grado di "pulire" il segnale e isolare le parti della traccia rilevanti per l'operazione.

[294] Cfr. A. Paoloni, *La voce come elemento di identificazione della persona*, in AA.VV., *La voce come bene culturale*, (a cura di) A. De Dominicis, Carocci, Roma, 2002, p. 129.

[295] In ambito giudiziario si procede sempre con i test di tipo "aperto" e la questione è più complessa in quanto il risultato di compatibilità non è risolutivo e l'unico approccio possibile risulta quello statistico. M. Biral, *L'identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, in *Rivista Italiana di Diritto e Procedura Penale*, 4, 2015, p. 1842.

[296] Cfr. M. Biral, *L'identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, in *Riv. It. di Dir. e Proc. Pen*., 4, 2015, p. 1842: «è di tutta evidenza come ci siano circostanze in cui è fondamentale stabilire a chi appartenga un determinato profilo vocale. Può accadere che l'autore di un reato non sia stato visto, ma ascoltato: si pensi a una rapina portata a segno da soggetti mascherati o al sequestro di persona con la vittima custodita in condizioni che non le permettano di vedere i suoi carcerieri. Oppure potrebbe sussistere la necessità di individuare uno o più degli interlocutori di una conversazione intercettata».

[297] Cfr. A. Bernasconi, *La ricognizione di persone nel processo penale*, Giappichelli, Torino, 2004, p. 9 e A. M. Capitta, *Ricognizioni e individuazioni di persone nel diritto delle prove penali*, Giuffrè, Milano, 2001, p. 89.

ed emozionale del soggetto[298], ve ne sono altre (cd. "esogene") legate al contesto percettivo. Diversi errori possono ricondursi a una bassa intensità dell'impressione uditiva, oppure a un'eccessiva distanza o frapposizione di ostacoli fra l'ascoltatore e la fonte di emissione. Ne consegue che l'atto del riconoscere risulta estremamente complesso e non così facilmente spiegabile nelle sue dinamiche profonde, essendo soggetto a errori difficilmente verificabili.

Nell'impianto codicistico, gli istituti giuridici di riferimento sono da sempre la ricognizione[299] e l'individuazione[300]. Il modello disegnato dal primo riferimento normativo guarda al dibattimento, ad una fase, cioè troppo avanzata del processo per garantire l'affidabilità della memoria[301]. Il riconoscimento soggettivo dovrebbe pertanto trovare il suo alveo naturale nelle indagini preliminari. Invero, la prassi giudiziaria è quella di ricorrere all'istituto dell'incidente probatorio, *ex* art. 392 comma 1 lett. *g*) c.p.p.[302]. Quanto all'individuazione, come noto costituisce un atto tipico del pubblico ministero, delegabile alla polizia giudiziaria, *ex* art. 370 c.p.p.. Trattasi di un'operazione probatoria che, dal punto di vista materiale, ha un valore elevatissimo, in quanto racchiude quel "primo" riconoscimento che rappresenta l'unico davvero attendibile. E' pur vero che gli esiti dell'attività ricognitiva in fase di indagini preliminari hanno un mero valore orientativo[303]. Tuttavia, sono frequenti le pronunce giurisprudenziali che qualificano l'individuazione come una *species* del *genus* dichiarazione, avente una forza probatoria legata allo stesso valore della dichiarazione[304]. Ne consegue che l'individuazione in tal modo acquista rilevanza ai fini della decisione sulla colpevolezza: l'istituto sembrerebbe fondersi così con la testimonianza come una sorta di fattispecie a formazione progressiva, nell'ambito della quale il momento cruciale è rappresentato proprio dal riconoscimento.

Capita poi molto spesso che, durante le operazioni di intercettazione l'attribuzione dell'identità di una voce sia effettuata direttamente dalla polizia giudiziaria: quest'ultima, infatti, oltre a verificare l'intestazione dell'utenza, la titolarità della scheda telefonica utilizzata, l'analisi dei tabulati telefonici,

---

[298] Cfr. M. Biral, *L'Identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, cit., p. 1842.

[299] L'art. 216 c.p.p. trova applicazione nei casi in cui si debba procedere a riconoscere «voci, suoni o quanto altro può essere oggetto di percezione sensoriale».

[300] In fase di indagine, l'identificazione della voce può essere acquisita ai sensi dell'art. 361 c.p.p.

[301] Essa risulta inversamente proporzionale al trascorrere del tempo. Cfr. C. Cesari, *Individuazione e dibattimento: limiti e rischi dell'uso a fini contestativi di un atto di indagine*, in *Critica al diritto*, 1995, p. 145, efficacemente osserva che: «è nella natura degli atti ricognitivi consumare in fretta le proprie energie».

[302] Sul punto, cfr. R. Dell'Anno, *Osservazioni in tema di individuazione e ricognizione di persona nel nuovo codice di procedura penale*, in *Cass. pen*., 1991, p. 1900, A. Sanna, *In tema di ricognizione personale mediante incidente probatorio*, in *Riv. it. di Dir. e Proc. Pen*. 1990, p. 1669, M. Tiberi, voce *Ricognizioni*, in *Dig. Disc. Pen. Agg*., vol. III, t. II, (a cura di) A. Gaito, Torino, 2005, p. 1426.

[303] Cfr. Corte Cost., 12.6.1991, n. 265, in *Giust. pen*. 1991, I, 225.

[304] Cfr. Cass. pen., Sez. II, 3.12.2013, n. 50954 in *CED Cass* n. 257985, Cass. pen., Sez. V, 21.10.2010, n. 43363 in *CED Cass* n. 248951, Cass. pen., Sez. VI, 5.12.2007, n. 6582 in *CED Cass* n. 239416, Cass. pen., Sez. II, 11.3.2004, n. 16204 in *CED Cass* n. 228777, Cass. pen., Sez. V, 6.4.1999, n. 12027 in *CED Cass* n. 214872.

può eseguire altresì l'identificazione della voce[305]. Si tratta di ipotesi piuttosto particolari, in cui potrebbe non essere opportuno procedere ad un'individuazione *ex* art. 361 c.p.p., perché potrebbe danneggiare l'attività investigativa in corso. Risulta tuttavia legittima - per la giurisprudenza maggioritaria - la testimonianza di un ufficiale di polizia chiamato a confermare il riconoscimento dell'indagato avvenuta mediante il timbro vocale[306].

Quanto poi al riconoscimento di carattere oggettivo, negli ultimi anni si stanno sempre più diffondendo sistemi automatici o semi-automatici, il cui effettivo funzionamento, però, come la maggioranza dei sistemi basati su processi automatizzati, risulta in buona parte oscuro[307]. Ad oggi, il metodo più utilizzato nelle aule giudiziarie è quello "parametrico"[308], ossia un approccio semi-automatico in cui viene distinta la voce di ciascun individuo sulla base di alcuni parametri dipendenti dalla conformazione anatomica dell'apparato fonatorio. Si tratta di un sistema semi automatico di riconoscimento biometrico che non sempre necessita di una successiva verifica del risultato da parte dell'operatore esperto[309].

---

[305]La giurisprudenza ritiene che costituisca valido indizio la dichiarazione dell'ufficiale che affermi di aver riconosciuto, ascoltando le registrazioni di conversazioni telefoniche, la voce dell'imputato, a lui familiare poiché nota per ragioni investigative o per altre circostanze. Cfr. Cass. pen., Sez. I, 8.5.2013, n. 35011 in *CED Cass* n. 257209; Cass. pen., Sez. I, 20.9.2007, n. 38484 in *CED Cass* n. 238042; Cass. pen., Sez. I, 6.3.2007, n. 22722 in *CED Cass* n. 236763; Cass. pen., Sez. II, 23.11.2004, n. 47673 in *CED Cass* n. 229909; Cass. pen., Sez. V, 27.10.2004, n. 11921 in *CED Cass* n. 231872.

[306] Al fine di verificare l'affidabilità di tali dichiarazioni si procede alla *cross examination* e, eventualmente, all'assunzione di una perizia o consulenza tecnica fonica. V. *ex multis* Cass. pen., Sez. II, 27.1.2017, n. 12858 in *CED Cass* n. 2699001 e Cass. pen., Sez. VI, 3.10.2013, n. 13085 in *CED Cass* n. 59478.

[307] Nonostante ciò, la trasposizione del riconoscimento vocale nell'ambito di processi automatici incontra il massimo grado di *gradimento* da parte degli utenti.

[308] «L'analisi tecnica è scandita da tre diversi momenti. In primo luogo, occorre scegliere, tra il materiale fonico disponibile, parole o frasi con determinate caratteristiche qualitative e quantitative. In particolare, il segnale deve essere intellegibile (non inquinato, cioè, dai rumori di fondo e non "mescolato" al segnale riconducibile ad altri soggetti) e deve avere una durata di almeno 20 secondi. Successivamente, si procede, con l'ausilio di appositi programmi, ad isolare, nell'ambito delle parole selezionate, le vocali a-e-i-o (non la u perché è meno frequente nella lingua italiana). Da queste si estraggono e si misurano i parametri più significativi per la caratterizzazione del parlatore: la frequenza fondamentale (FF0) e le formanti (FF1, FF2, FF3, FF4). La FF0 è la frequenza più bassa presente nella voce ed è legata alle caratteristiche anatomiche del parlante e al suo atteggiamento fonatorio. Le formanti, invece, sono le zone dello spettro vocale in cui risulta massima l'energia sonora. Infine, il programma svolge l'analisi statistica dei risultati e il confronto fra i valori ottenuti per il campione dell'anonimo e quello dell'indiziato (o, più in generale, del riconoscendo)». M. Biral, *L'identificazione della voce nel processo penale*, cit., p. 1842.

[309] Ad oggi, i risultati di altri sistemi automatici di riconoscimento biometrico (per es. volto o impronte digitali) sono nella prassi sempre oggetto di verifica da parte di un operatore esperto che ha, tra l'altro, il compito di controllare la compatibilità o meno fra i due *templates* confrontati. Questo in ragione del fatto che i risultati non si esprimono in termini di *likelihood ratio*, ossia di "rapporto di verosimiglianza" (relazione fra il valore di similarità e tipicità), in base ad una popolazione di riferimento (v. il § 3.3.1 sul funzionamento della bancadati A.F.I.S.). Il rapporto di verosimiglianza (*LR*) è il rapporto tra la *similarità* dei campioni a confronto, ovvero quanto risulta simile il campione noto rispetto a quello anonimo (al numeratore) e la *tipicità*, ovvero quanto il campione in esame sia comune in una data porzione di popolazione di riferimento (al denominatore). I risultati di alcuni sistemi automatici di riconoscimento non calcolano automaticamente la verosimiglianza del dato di un determinato soggetto indagato corrispondente a quello del soggetto ignoto. Al contrario, forniscono una previsione basata su una comparazione di informazioni del singolo indagato/imputato rispetto a quelle di un gruppo di soggetti simili. Su questo punto v. per es. con riferimento al riconoscimento facciale, *Best Practice Manual for Facial Image Comparison*, pubblicate dall'ENFSI-BPM-DI-01 Version, 01 - 2018, reperibili all'indirizzo https://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf (visualizzato in data 28.7.2021).

Per quanto riguarda l'affidabilità delle indagini foniche compiute mediante perizia o consulenza tecnica, la giurisprudenza è stata piuttosto altalenante[310]. Particolare interesse ha destato una vicenda giudiziaria in cui è stato applicato per la prima volta un sistema automatico, denominato *Speaker Recognition System*[311]. La Cassazione ha desunto l'affidabilità dell'indagine fonica dal fatto che il software avesse compiuto un'oggettiva comparazione dei due dati a disposizione (una voce precedentemente intercettata e quella appartenente all'imputato), escludendo interpretazioni meramente soggettive[312]. Invero, l'oggettività non può costituire di per sé una garanzia di qualità: il rischio che si corre è quello di affidarsi ciecamente a metodi il cui funzionamento risulti oscuro e la cui attendibilità non possa di fatto essere verificata[313]. Inoltre, in quell'occasione, il giudice non sembra essersi interrogato sul tipo di software impiegato[314]: il rilievo, come si approfondirà meglio

---

Il riconoscimento vocale automatico o semi-automatico avviene, invece, con le seguenti modalità: «se si sfruttano tecniche automatiche o semi-automatiche bisogna stabilire una misura di distanza o di dissimilarità tra parlatori; viene quindi stimata la distribuzione della distanza del parlatore anonimo da se stesso e la distribuzione della distanza dell'anonimo da tutti gli altri parlatori inseriti in una Base-Dati di confronto che si possa considerare rappresentativa della popolazione di riferimento cui si ritiene appartenga la voce dell'anonimo. Sulla base di tali distribuzioni si definisce un valore soglia, che identifica il criterio di decisione. Infine, confrontando la distanza tra voce anonima e voce dell'indiziato con tale soglia, si stabilisce se le due voci sono uguali o diverse, avendo definito a priori il criterio di decisione (scelta di un valore massimo ammissibile per l'errore di seconda specie, scelta di un livello fissato per il rapporto di verosimiglianza…)». T. Bove, P. E. Giua, A. Forte, C. Rossi, *Un metodo statistico per il riconoscimento del parlatore basato sull'analisi delle formanti*, in *Statistica*, anno LXII, n. 3, 2002, p. 480.

[310] Il metodo parametrico è stato ritenuto talvolta dotato di un'elevatissima capacità identificativa (cfr. *ex multis* Cass. pen., Sez. V, 9.7.1993, n. 8416 in *CED Cass* n. 196264), altre volte non è stato ritenuto affidabile (cfr. Cass. pen., Sez. VI, 16.2.2020, n. 18708, *inedita*, Cass. pen., Sez. IV, 4.7.2017 n. 43871, *inedita*). Dello stesso avviso P. Rivello, *Tecniche scientifiche e processo penale*, in *Cass. pen*., fasc. 4, 2013 p. 1691B.

[311] Elaborato da una società russa (*Speech Technology Center*, con sede in San Pietroburgo, creata nel 1990) come metodo automatico di identificazione vocale, utilizzando il programma *voice-net*, che permette la comparazione della voce nota anche se si dispone di un campione di soli 16 secondi di durata. Il metodo permette il confronto in automatico dei suoni più che delle parole con la conseguenza che è possibile utilizzare anche il parlato avente un significato incomprensibile.

[312] Cass. pen., Sez. II, 11.7.2012, n. 40611 in *CED Cass* n. 254344.

[313] Per un approfondimento sull'approccio scientifico generalmente utilizzato v. G. S. Morrison et al., *Consensus on validation of forensic voice comparison*, in *Science & Justice*, vol. 61, 3, 2021, pp. 299-309.

[314] In merito al software utilizzato la Cassazione si esprime nei seguenti termini: «(…) nella prima consulenza tale campione è stato messo a confronto con un saggio proveniente da un'intercettazione che era stata disposta nel 2000, a carico del fratello dell'imputato, nel corso della quale fu captata una conversazione del ricorrente con la madre. Non erano disponibili saggi più recenti perché l'ARZU si era reso latitante fin dal 2002. Il programma informatico ha confermato l'elevata probabilità che l'ignota voce registrata a Perugia il 14 aprile 2007 fosse dell'ARZU. In particolare il programma ha dato come risultato della probabilità di errore nel caso che la voce fosse attribuita alla stessa persona ("falsa accettazione") una percentuale del 4,32% quindi minima, mentre l'errore sulla probabilità che la voce fosse attribuita a persone diverse ("falso rifiuto" è risultato notevolmente maggiore 30,28%). Nella seconda consulenza, effettuata dopo che il ricorrente, in sede di perizia disposta dal tribunale, aveva rilasciato un saggio fonico, il programma ha dato come risultato una percentuale più elevata del "falso rifiuto" (31,66%) a fronte di una percentuale più bassa (1,36%) della "falsa accettazione". La probabilità di errore che la voce intercettata fosse dell'ARZU è stata ritenuta dal sistema estremamente bassa.
I giudici di merito hanno ritenuto il metodo attendibile perché, in aggiunta ai riconoscimenti vocali soggettivi, compresi quelli effettuati dalla polizia giudiziaria che ha fatto riferimento al particolare timbro di voce che rendeva l'imputato riconoscibile, il sistema aveva effettuato una oggettiva comparazione dei dati interamente affidata al software, escludendo interpretazioni meramente soggettive.
Il valore probatorio attribuito alla conclusione peritale (e indipendentemente dai riconoscimenti soggettivi effettuati dalla polizia giudiziaria), realizzata a seguito di affidabile metodologia di ricerca, risulta, pertanto, incensurabile». Cass. pen., Sez. II, 11.7.2012, n. 40611 in *CED Cass* n. 254344.

infra[315], non è di poco conto, dal momento che l'utilizzo di sistemi dei quali siano noti, o quantomeno individuabili, gli algoritmi rappresenta un primo passaggio fondamentale per un controllo effettivo sull'affidabilità dei risultati.

Con riferimento al peso probatorio da accordare ai risultati dell'indagine fonica, infine, occorre soffermarsi su alcune riflessioni. Come già rilevato *supra*, la traccia fonica costituisce un bioindicatore che non consente di risalire in modo certo al soggetto titolare.

Per tale ragione, alcune pronunce hanno attribuito alle indagini foniche un valore meramente indiziario: è necessario, quindi, che ai risultati della prova tecnica si affianchino sempre elementi di riscontro, suscettibili di collegare l'imputato al fatto di reato contestatogli. Quanto al rapporto fra l'approccio all'impronta fonica soggettivo ovvero oggettivo, non è possibile affermare in modo netto che una metodologia sia più efficiente dell'altra[316]. Il giudice, caso per caso, stabilisce in sede di valutazione della prova come "ponderare" i risultati dell'apprezzamento soggettivo rispetto a quelli dell'accertamento tecnico, qualora avessero dato risultati divergenti.

3.5.2. L'andatura del passo

Fra i sistemi di riconoscimento dinamici, rientrano altresì le tecniche di identificazione basate sull'andatura del soggetto[317]. L'analisi di questa avviene per mezzo di una telecamera che riprende la specifica modalità con cui l'interessato cammina, misurando la forma, la dinamica del corpo, l'andatura delle gambe, la cadenza e la velocità del passo. Ad oggi, il metodo si basa su diverse analisi antropometriche eseguite direttamente da operatori esperti[318]. A partire dall'ultimo decennio, si stanno

[315] Cfr. il capitolo II, §§ 2 e ss.

[316] Cfr. K. La Regina, *L'identificazione della voce nel processo penale*, cit., pp. 88 e ss.

[317] Cfr. S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, cit., p. 36.

[318] Per l'esecuzione di tale analisi dinamica, si è soliti ricorre allo strumento della perizia (artt. 220 e ss. c.p.p.) o della consulenza tecnica di parte (art. 225 c.p.p.). A tal proposito, particolare interesse ha destato la pronuncia della Corte d'Appello d'Assise di Torino (n. 21 del 22.02.2016) in cui sono state riportate alcune parti rilevanti di relazioni tecniche eseguite dai consulenti tecnici delle parti, aventi ad oggetto la misurazione antropometrica dell'andatura dell'imputato. Più nel dettaglio, nella prima relazione datata 26.7.2012, il Professor Lingua, consulente tecnico del p.m., ha esposto la particolare metodologia adottata per acquisire la sincronizzazione della velocità del passo e la misurazione degli specifici dettagli antropometrici dell'attentatore. In una successiva relazione (17.1.2013), nel comparare le andature rispettivamente dell'imputato e dell'attentatore, il consulente ha rilevato: «un atteggiamento in valgismo di ginocchio e piede bilateralmente. L'appoggio del piede avviene con il calcagno in pronazione. La deambulazione avviene con tempo di carico minore a destra cui consegue una apparente zoppia. Si osserva un'asimmetria delle spalle, con la destra che appare abbassata rispetto alla sinistra». Quanto all'attentatore, invece, «l'osservazione del filmato evidenzia un atteggiamento in valgo di entrambi i piedi (le ginocchia non sono visibili perché coperte dal cappotto), con atteggiamento di pronazione del calcagno. Si apprezza una visibile zoppia per diminuzione del tempo di contatto a terra del piede destro. La spalla destra è più bassa e lievemente retro posta rispetto alla sinistra. La retro posizione della spalla è peraltro più che verosimilmente da porre in relazione con il fatto che il braccio sinistro è lievemente avanzato in quanto sostiene un pacco». Il consulente ha concluso, in tal modo, sostenendo la coincidenza fra la figura dell'attentatore e dell'imputato, in quanto entrambi «presentano una anomalia nella dinamica del passo per cui si verifica un appoggio a terra del piede destro di durata apprezzabilmente minore di quanto avviene per il piede sinistro». La sentenza della Corte d'Assise d'Appello è stata confermata dalla pronuncia della Corte di cassazione [Cass. pen., Sez. I, 1.2.2018 n. 41514, *inedita*].

sempre più diffondendo diversi studi aventi ad oggetto algoritmi di determinazione delle relazioni matematiche che intercorrono fra diverse parti del corpo[319]. Tuttavia il principale limite nell'impiego di sistemi automatici o semi-automatici di riconoscimento dell'andatura risiede nella costruzione di un database centralizzato per la fase di *matching*. Per tale ragione, ad oggi non è ancora possibile eseguire delle comparazioni automatiche sull'andatura dei soggetti: in questo caso, infatti, le misurazioni antropometriche avvengono in modalità del tutto analogica da parte di operatori esperti di anatomia e ortopedia.

3.5.3. Il riconoscimento dinamico della firma

Le peculiarità della firma autografa rientrano nel generale novero delle caratteristiche biometriche comportamentali e vengono raccolte tramite speciali "tavolette di acquisizione" (cd. *tablet* grafometrici), dotate di sensori e programmi software[320]. I dispositivi utilizzati sono in grado di rilevare, oltre al tratto grafico, anche una serie di caratteristiche dinamiche associate all'atto della firma (velocità di tracciamento, accelerazione, pressione, inclinazione, etc…). L'acquisizione dei tratti dinamici della firma risulta funzionale a procedure di autenticazione più che di identificazione, in quanto tali sistemi di riconoscimento presentano un tasso ancora piuttosto elevato di falsi negativi che li rendono poco efficienti e imprecisi, fuori da contesti in cui sia possibile sopperire con l'intervento umano agli inevitabili errori di riconoscimento. Tuttavia, analogamente a quanto accade per i sistemi di riconoscimento basati sull'andatura, è possibile ricorrere alla perizia o alla consulenza tecnica per la misurazione in via analogica del tratto biometrico considerato, a cui l'orientamento maggioritario della Corte di cassazione riconosce in ogni caso un valore meramente indiziario[321].

3.6. Cenni in materia di genetica forense

Nel § 2 si è fatto cenno a quello che si potrebbe definire cd. "ciclo della prova biometrica", illustrando quali sono i principali passaggi che interessano la trasformazione dal corpo "fisico" al

[319] Sul punto cfr. *ex multis* A.R. El Khobby, H.A.M. Abd Elnaby, et al., *Gait identification by convolutional neural networks and optical flow*, in *Multimed Tools Appl* 78, 2019, pp. 25873-25888.

[320] Ad oggi, non sono utilizzati sistemi automatici o semi-automatici di identificazione (1:N, 1:N+1) in quanto non è ancora stato creato un database per i procedimenti di comparazione. Per una panoramica generale sul sistema di riconoscimento cfr. S. Agostinis, B. Catenacci, *Crimini e scrittura. La perizia grafica negli Stati Uniti*, Aras, Pesaro-Urbino, 2012, pp. 14 e ss. e A. Bravo, *Argomenti di Grafologia peritale*, E.S.I. Napoli, 2001, A. Bravo, *Variazioni naturali e artificiose della grafia*, Giordano Editore, Mesagne, 2005, A. Bravo, *Metodologia della consulenza tecnica e della perizia grafica*, Giordano Editore, Mesagne, 2005, S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, cit., p. 38.

[321] Cfr. Cass. pen., Sez. V, 13.2.2017, n. 18975 in *CED Cass* n. 269908, Cass. pen., Sez. V, 14.04.1999, n. 10363 in *CED Cass* n. 214188; Cass. pen., Sez. V, 23.10.1990, n. 15852, in *CED Cass* n. 185898.

corpo "elettronico". Come visto, ciascun sistema di riconoscimento biometrico presenta determinate caratteristiche ontologiche che risultano molto diverse rispetto agli altri strumenti di identificazione o di autenticazione, soprattutto in relazione allo specifico contesto giudiziario. Oggetto di questa parte della ricerca sarà una breve ricostruzione del rapporto intercorrente tra l'analisi del Dna e il procedimento penale: in particolare giova dar conto, a fronte dell'amplissima e approfondita letteratura, dello stato dell'arte in ordine all'impiego di questa particolare categoria di dato biometrico[322] nell'ambito del processo penale[323]. Si ritiene doveroso premettere che per gli scopi che

[322] L'analisi del Dna è stata recentemente ammessa tra le tecnologie biometriche che sono all'attenzione del sub-comitato di standardizzazione ISO (ISO/IEC JTC1SC 37 "*Biometrics*") anche se, a differenza di altre tecniche di riconoscimento, non permette un'autenticazione/identificazione in tempo reale. Quest'ultimo criterio, però, non è contemplato in nessuna delle diverse definizioni di tecnologie biometriche e quindi non impedisce di annoverare l'analisi e la comparazione del Dna tra le stesse. A. Jain, *Biometrics: Past, Present and Future*, in *18th IAPR/IEEE Int.l Summer school for advanced studies on biometrics: BIOMETRICS FOR AI / AI FOR BIOMETRICS*, 2021 e COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, reperibile in http://bioetica.governo.it/media/1846/p95_2010_identificazione-corpo-umano-biometria_it.pdf (ultimo accesso il 10.1.2021). Il regolamento (UE) 2016/679 e la direttiva 2016/680/UE distinguono i dati genetici dai dati biometrici. In particolare, i dati genetici sono i «dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione» (art. 4, par. 13 GDPR e art. 3, par. 12 LED), e, se sottoposte a determinati trattamenti tecnici specifici, consentono o confermano il riconoscimento, ovvero, impiegando la criticata terminologia del regolamento (cfr. *supra* il § 1), l'identificazione univoca degli individui. Ne consegue che, quando i dati genetici, sottoposti ad un "trattamento tecnico specifico" sono impiegati al fine di riconoscere una determinata persona fisica, essi possono essere annoverati fra i dati biometrici.

[323] Senza pretese di esaustività cfr. B. Lavarini, *Elementi di procedura penale. Lezioni per il corso di laurea magistrale in chimica clinica, forense e dello sport*, Ecig Universitas, Genova, 2010, pp. 139 e ss., C. Fanuele, *Dati genetici e procedimento penale*, Cedam, Milano, 2009, A. Scarcella, *Prelievo del Dna e banca dati nazionale*, Cedam, Milano, 2009, C. Fanuele, *La prova del Dna*, in AA.VV. *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Luparia, Cedam, Milano, pp. 587 e ss., P. Felicioni, *Considerazioni sul prelievo di materiale biologico dall'imputato*, in AA.VV. *La prova scientifica nel processo penale*, (a cura di) L. De Cataldo Neuburger, Cedam, Padova, 2007, pp. 383 e ss., P. Felicioni, *La prova del Dna: profili giuridici*, in AA.VV., *Scienza e processo penale: linee guida per l'acquisizione della prova scientifica*, (a cura di) L. De Cataldo Neuburger, Cedam, Padova, 2010, pp. 408 e ss., A. Santosuosso, *Diritto, scienza e nuove tecnologie*, Cedam, Lavis, pp. 122 e ss., T. Alesci, *Il corpo umano come fonte di prova*, cit., pp. 142 e ss., A. Andreoli, *Identità alla prova: la controversa storia del test del Dna, tra crimini, misteri e battaglie legali*, Sironi, Milano, 2009, pp. 43-45, U. Ricci, *Dna e crimine: dalla traccia biologica all'identificazione genetica*, Laurus Robuffo, Roma, pp. 108 e ss., A. Fiori, *Mito, realtà e fallacie del Dna (nella pratica forense)*, in *Rivista Italiana di Medicina legale e diritto sanitario*, fasc. 6, 2011, p. 1329, G. Novelli, I. Pietrangeli, M. Biancolella, A. Cammarano, G. Arcudi, *Le banche dati forensi: aspetti etici e di privacy*, in AA.VV., *Genetica forense e diritto: prospettive scientifiche, tecnologiche e normative*, (a cura di) M. Dobosz, E. Carnevali, M. Lancia, Giuffrè, Milano, 2011, pp. 47 e ss., P. Fattorini, F. Corradi, U. Ricci, C. Previderè, *La prova del Dna per la ricerca della verità. Aspetti giuridici, biologici e probabilistici*, Giuffrè, Milano, 2006, pp. 410 e ss., P. Felicioni, *Acquisizione di materiale biologico a fini identificativi o ricostruttivi*, in AA.VV., *Prelievo del Dna e banca dati nazionale*, (a cura di) A. Scarcella, Cedam, Milano, 2009, pp. 218 e ss., C. Gabrielli, *La decisione del "prelievo" torna al giudice*, in *Guida dir*., 2009, n. 30, p. 68, L. Scaffardi, *Banche dati del Dna e scambio internazionale fra esigenze securitarie e tutele dei cittadini*, in AA.VV., *La Banca dati italiana del Dna. Limiti e prospettive della genetica forense*, (a cura di) L. Scaffardi, Il Mulino, Bologna, 2019, pp. 13 e ss., L. Luparia, *Prova genetica e Banca dati nazionale. Quali sfide per il processo penale contemporaneo*, in AA.VV., *La Banca dati italiana del Dna. Limiti e prospettive della genetica forense*, (a cura di) L. Scaffardi, Il Mulino, Bologna, 2019, pp. 27 e ss., G. Canzio, *Prova del Dna e processo penale: punti fermi…e non*, in AA.VV., *La Banca dati italiana del Dna. Limiti e prospettive della genetica forense*, (a cura di) L. Scaffardi, Il Mulino, Bologna, 2019, pp. 157 e ss., P. Tonini, *Accertamento del fatto e informazioni genetiche: un difficile bilanciamento*, in *Diritto penale e processo*, 2009, pp. 1 e ss., E. Stefanini, *Dati genetici e diritti fondamentali*, Cedam Padova, 2008, pp. 164 e ss., V. Marchese, L. Caenazzo, D. Rodriguez, *Banca dati nazionale del Dna: bilanciamento tra diritti individuali e sicurezza pubblica nella legge 30 giugno 2009, n. 85*, in *Rivista Italiana di Diritto e Procedura Penale*, fasc.4, 2013, p. 1863, P. Felicioni, *La prova del DNA: profili giuridici*, in AA.VV., *La prova scientifica nel processo penale*, (a cura di) Tonini P., supplemento a *Dir. pen. proc*., n. 6, 2008, p. 52, A. Musumeci, *La ratifica del Trattato di Prüm*, in AA.VV., *Banca dati del DNA e accertamento penale*, (a cura di) L. Marafioti, L. Luparia, Giuffrè,

interessano la presente ricerca non è possibile approfondire esaustivamente l'evoluzione che ha portato al progresso attuale della genetica forense. S'intende infatti qui ripercorrere solamente le principali questioni che interessano la materia nell'attuale periodo storico nonché i fondamentali passaggi del procedimento di digitalizzazione biometrico del Dna (cfr. *supra* il § 2.2).

Negli ultimi anni, tale sistema di riconoscimento ha assunto sempre più importanza, anche grazie all'affermazione di nuove tecnologie che consentono di estrarre un profilo genetico non solo da campioni biologici "tradizionali" (sangue, saliva, liquido seminale ecc.), ma anche da ridottissime quantità di materiale organico rinvenute sulla *scena criminis*[324].

Come noto, per Dna (acido desossiribonucleico) s'intende la molecola, composta da un lungo polimero costituito a sua volta da una catena di basi azotate, depositaria dell'informazione genetica. Tale molecola rappresenta, da tempi ormai risalenti, uno dei principali strumenti identificativi esistenti in quanto si trova presente in tutte le cellule umane ed è altamente *individualizzante*, perché non esistono due soggetti geneticamente identici[325]. Più nel dettaglio, oggetto dell'analisi finalizzata all'identificazione personale è il "polimorfismo" del Dna[326], ossia la parte "intronica" della suddetta molecola[327]. Grazie a questa, attraverso un test[328] è possibile confrontare le caratteristiche del Dna

---

Milano, 2010, pp. 13 ss., M. Corasaniti, *La banca dati del DNA: primi aspetti problematici dell'attuazione del Trattato di Prum*, in *Dir. informatica*, fasc.3, 2009, p. 437, A. Camon, *La prova genetica tra prassi investigative e regole processuali*, in *Proc. pen. giust*., 2015, n. 6, pp. 165 e ss.

[324] Le cd. "tracce da contatto" ottenute da oggetti che sono stati toccati anche per breve tempo. Sul punto cfr. U. Ricci, *Limiti e aspettative della genetica forense*, in AA.VV., *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, (a cura di) C. Conti, Giuffrè, Milano, 2011, p. 254. L'art. 6 della legge n. 85 del 2009 (cfr. *infra* il § 3.6.2) definisce il "*campione biologico grezzo*" come la «quantità di sostanza biologica prelevata sulla persona sottoposta a tipizzazione del profilo del DNA», distinto dal "*reperto biologico*" definito come «materiale biologico acquisito sulla scena di un delitto o comunque su cose pertinenti al reato».

[325] Eccetto i gemelli omozigoti, cfr. AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze, logica*, cit., pp. 679 e ss. e C. Fanuele, *L'indagine genetica nell'esperienza italiana ed in quella inglese*, in *Riv. it. dir. proc. pen*., 2006, pp. 732 e ss.

[326] Giova ricordare che la scoperta del primo polimorfismo del Dna si deve ad Alec Jeffreys, nel 1985. Cfr. A. J. Jeffreys, V. Wilson, S. L. Thein, *Individual-Specific 'Fingerprints' of Human DNA*, in *Nature*, vol. 316, 1985. Il metodo di Jeffreys fu successivamente migliorato e pochi anni dopo, le tecniche di Dna *profiling* si sono arricchite grazie all'esame dei loci polimorfici STR (*Short Tandem Repeat*), mentre alla fine del secolo si è arrivati all'introduzione dei sequenziatori ed analizzatori di frammenti, automatici, per la contemporanea tipizzazione fino a 16 loci, con l'individuazione anche del sesso. Per una rassegna esaustiva sulle tecniche utilizzate nell'ambito della genetica forense (inclusi gli esami relativi al Dna mitocondriale e al cromosoma Y, rispettivamente per le identificazioni per linea materna e i profili maschili), si rimanda a F. Alessandrini, *Statistica applicata all'esame dei polimorfismi del Dna*, in AA. VV., *Introduzione alla Genetica Forense*, (a cura di) A. Tagliabracci, Milano, Springer, 2010, pp. 119 ss. e COUNCIL OF BIOETHICS, *The forensic use of bioinformation: ethical issues*, Cambridge, Cambridge Publisher, 2007. Per una ricostruzione storica cfr. AA.VV., *L'investigazione scientifica e criminologica nel processo penale*, (a cura di) Cedam, Padova, 1989, p. 63.

[327] In questi termini cfr. A. Fiori, *L'identificazione genetica: il DNA*, in AA.VV., *L'investigazione scientifica e criminologica nel processo penale*, Padova, Cedam, 1989, p. 63.

[328] Per un approfondimento sul metodo scientifico utilizzato per l'analisi del Dna v. A. Gargani, *I rischi e le possibilità dell'applicazione dell'analisi del Dna nel settore giudiziario*, in *Riv. it. dir. proc. pen.*, 1993, p. 1310. Il metodo più diffuso oggi è basato sull'estrazione del materiale genetico contenuto nel nucleo cellulare (nDna) e quello contenuto nei mitocondri (mtDna) dalle componenti proteiche ed è costituito da quattro fasi. La prima consiste nella rottura delle membrane (lisi cellulare), cui segue la degradazione o precipitazione delle proteine e di altri componenti cellulari. La terza fase consiste poi nell'isolamento del Dna

ricavate dalle tracce biologiche[329] rilevate sulla *scena criminis* con quelle dell'indagato/imputato. Tuttavia, sebbene nella prassi giudiziaria le analisi generali in laboratorio siano considerate le più affidabili in termini di attendibilità[330], nell'ambito della genetica forense i casi di contaminazione probatoria o errori di manipolazioni costituiscono un costante rischio da mettere in conto[331]. Ne consegue l'importanza di soffermarsi su ciascuna "fase" dell'indagine genetica al fine di comprendere la potenziale attendibilità del risultato.

3.6.1. Dalla "repertazione" del campione biologico grezzo alla sua conversione in *template*

Come noto, la polizia giudiziaria può compiere accertamenti e rilievi durante la prima fase dell'esame della scena del crimine[332]. È tale la cd. "repertazione", ossia la raccolta, la custodia e la conservazione di tutto ciò che può avere un collegamento con il fatto di reato[333]. Tali operazioni si giustificano con ragioni di urgenza la cui esistenza è necessaria per il contemperamento di due fondamentali esigenze: quella investigativa da un lato e la libertà personale dei soggetti coinvolti dall'altro[334]. Con particolare riferimento alla raccolta di tracce organiche da cui è possibile estrarre il Dna, tale operazione viene generalmente ricondotta nell'ambito delle attività che la polizia giudiziaria è legittimata a compiere *ex* art. 354 c.p.p.[335]. Pertanto, nell'alveo dei rilievi eseguibili dalla polizia

---

e la quarta nella purificazione. Sul punto cfr. C. Ricci, Previderè, P. Fattorini, F. Corradi, *La prova del Dna per la ricerca della verità. Aspetti giuridici, biologici e probabilistici*, Giuffrè, Milano, 2006, pp. 124 e ss.

329 La nozione di "materiale biologico" è da rinvenire nell'art. 6 co. 1 lett. *c*) l. 22.2.2006, n. 78, di attuazione della direttiva 98/44/CE, che lo definisce come «il materiale contenente informazioni genetiche, autoriproducibile o capace di riprodursi in un sistema biologico».

330 Sottolinea C. Canzio, *Prova scientifica, ricerca della "verità" e decisione giudiziaria nel processo penale*, in AA.VV., *Scienza e casualità*, (a cura di) C. De Maglie, S. Seminara, Cedam, Padova, 2006, p. 145, come: «la misurazione oggettiva e quantitativa dei risultati ottenuti tramite le sempre più sofisticate tecniche investigative, in numerosi casi non appaia uniforme e incontroversa, sicché la contrastata attendibilità della base cognitiva non risolve lo stato di incertezza probatoria né i nodi della decisione giudiziaria».

331 Cfr. J. Freckleton, *Problems posed by Dna evidence: of blood, babies and bathwater*, 17 (1), *Alternative Law Journal*, 10, 1992.

332 Cfr. il § 2. Gli ufficiali di polizia giudiziaria hanno la facoltà di accedere alla scena del crimine per eseguire accertamenti e rilievi «se il pubblico ministero non può intervenire tempestivamente o non ha ancora assunto la direzione delle indagini» (art. 354 c. 2 c.p.p.). Giova ricordare che cosa si intenda per "esame della scena del crimine", a tal proposito cfr. D. Curtotti, L. Saravo, *Manuale delle investigazioni sulla scena del crimine*, cit., p. 45, ove è definito come «quel complesso di attività poste in essere dalla polizia giudiziaria, dal consulente tecnico, dal pubblico ministero e dalla difesa, aventi natura tecnica e scientifica, esperibili sul *locus commissi delicti*, sia nell'immediatezza della scoperta del fatto di reato che nell'esecuzione di eventuali successivi accessi, finalizzate ad isolare, descrivere e analizzare lo scenario, nonché ricercare, esaminare e repertare le tracce ivi rinvenute».

333 «Il prelievo di materiale biologico è altra cosa rispetto alla raccolta e all'acquisizione di tracce biologiche. Queste possono essere trovate in luoghi, su cose, su cadaveri». D. Curtotti, L. Saravo, *Manuale delle investigazioni sulla scena del crimine*, cit., p. 70.

334 Peraltro, non è necessaria la presenza del difensore, il quale comunque conserva il diritto di assistere alle operazioni pur non dovendo essere preventivamente avvisato (art. 356 c.p.p.).

335 Cfr. S. Lorusso, *L'esame della scena del crimine tra esigenze dell'accertamento, istanze difensive e affidabilità dei risultati*, in AA.VV., *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, (a cura di) C. Conti, Giuffrè, Milano, p. 43. I rilievi si distinguono dalle ispezioni personali in quanto i primi riguardano l'aspetto esteriore della persona, mentre i secondi si concretizzano in accertamenti incidenti sulla libertà fisica o morale (tali il prelievo ematico, i rilievi su parti interne e comunque

giudiziaria, è ricondotto il rilevamento di reperti biologici eventualmente ottenuti da tracce biologiche lasciate casualmente, nonché quelli "abbandonati" e rinvenuti in sede di perquisizione (per esempio capelli caduti, mozziconi di sigaretta, ecc.)[336]. Tali tracce rientrano nelle "cose pertinenti al reato"[337], sequestrabili dalla polizia giudiziaria, anch'esse senz'altro utili per l'accertamento dei fatti. In altre parole, l'attività di "repertazione" rientra, sotto il profilo sistematico, tra le operazioni di polizia giudiziaria aventi carattere materiale ed esecutivo, prive, dunque, di qualsiasi carattere di invasività ed estranee alla categoria degli accertamenti tecnici, i quali, invece, implicano sempre una valutazione critica dei risultati ottenuti attraverso la loro disamina[338].

La fase di "repertazione" costituisce un momento fondamentale per la trasformazione del campione grezzo nel relativo *template*. Ciò in ragione del fatto che inidonee modalità di rilevamento ovvero una non corretta conservazione delle tracce biologiche incidono in modo rilevante sull'attendibilità delle successive analisi tecnico-scientifiche[339]. Occorre però sottolineare come l'evoluzione tecnologica degli ultimi anni, che ha messo a disposizione degli organi inquirenti strumenti di indagine sempre più all'avanguardia, non vada di pari passo con la ricettività da parte del diritto[340]. Di talché, la "tracciabilità" del percorso della raccolta del reperto dalla *scena criminis* fino al processo, non risulta ancora del tutto specificata dai protocolli tecnici[341]. Solo con il d.P.R. 7.4.2016 n. 87 è stato introdotto un sistema di accreditamento europeo dei laboratori di genetica forense destinati alle analisi molecolari

non normalmente esposte del corpo). Ne consegue che, i rilievi dattiloscopici, antropometrici e descrittivi non comportano alcun tipo di compressione della libertà personale. C. Fanuele, *La prova del Dna*, in AA.VV., *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Luparia, Cedam, Padova, 2018, pp. 594 e ss.

[336] Così, C. Fanuele, *I reperti organici sulla persona dell'indagato*, in *Cass. pen*., 2008, p. 3370 e AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze, logica*, cit., p. 17 ove si commenta la pronuncia della Corte. Cost., 15.11.2017, n. 239, in *Proc. pen*., 2018, p. 486, la quale ha escluso dal novero delle attività investigative di carattere tecnico-scientifico per le quali è prevista, a pena di nullità, la presenza del difensore e del consulente tecnico *ex* art. 360 c.p.p., i rilievi e i prelevamenti di reperti utili per la ricerca di tracce biologiche che però continuano a poter essere compiuti dai soli esperti della p.g. o dai consulenti tecnici del p.m.

[337] Così, Cass. pen., Sez. II, 13.3.2007, n. 12929, in *Guida dir*., 2007, n. 18, p. 96.

[338] Cfr. Cass. pen., Sez. I, 20.3.2013, n. 17645 in *CED Cass* n. 256237, Cass. pen., Sez. IV, 14.10.2008, n. 48415 in *CED Cass* n. 242385, Cass. pen., Sez. V, 24.1.2003, n. 9998, in *Cass. pen.*, 2004, p. 2453.

[339] Cfr. sul punto S. Lorusso, Investigazioni scientifiche, verità processuale ed etica degli esperti, in *Dir. pen. proc*., 2010, p. 1345.

[340] Si concorda con l'idea di un nuovo paradigma investigativo di D. Curtotti, L. Saravo, *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze, logica*, cit., p. 16-17: «si è convinti di due cose: a) anche per la prova proveniente dalla scena del crimine restano indispensabili le garanzie; b) per cercare di risolvere gli attuali problemi, non si può fare a meno di comprendere i nuovi sviluppi investigativi. La complessa vicenda della "prova scientifica" insegna che i mutamenti del mondo della tecnologia e delle scienze devono influire sull'interpretazione delle norme ed eventualmente anche sulla loro modifica. Diversamente, il codice rischia di divenire ben presto obsoleto a danno dei diritti dell'imputato e della collettività. Allo stesso tempo, non va sottaciuto che: a) molte delle regole comuni in punto di prova possano essere applicate alla prova di carattere scientifico, soprattutto in tema di valutazione; b) il rispetto formale delle garanzie (…) non esime il giudice dal controllo della affidabilità scientifica del risultato di prova. In tema di prova scientifica, al pari di tutte le altre prove, la forma non può mai prevalere sulla sostanza».

[341] Cfr. C. Fanuele, *La prova del Dna*, cit., p. 597. Il codice infatti prevede solo un obbligo di documentazione con specifico verbale delle operazioni svolte (art. 357 c.p.p.) e la facoltà del difensore di assistere alle operazioni, senza diritto di preavviso (art. 356 c.p.p.). Cfr. anche D. Curtotti, L. Saravo, *Manuale delle investigazioni sulla scena del crimine*, cit. p. 56.

per l'individuazione dei profili genetici (UNI ISO/IEC 17025)[342]. Tale riconoscimento formale assicura che l'analisi del Dna sia effettuata in conformità ai più elevati standard qualitativi per garantire l'attendibilità del risultato[343]. Al fine di tutelare il più possibile l'idoneità identificativa e la qualità dei profili, è stato previsto che siano inseriti nella banca dati nazionale del Dna solamente i *template* dei profili ottenuti con metodi accreditati tramite tale specifico sistema[344] (art. 10, co. 4, reg. att.). Tuttavia, in accordo con la maggioranza della dottrina[345], si ritiene che, rispetto all'attività di prelevamento, conservazione e trasmissione delle tracce pertinenti al reato, risulti ancora insufficiente la disciplina codicistica delle attività urgenti attuabili dalla polizia giudiziaria. Su tale aspetto il d.P.R. tace: di conseguenza, potrà accadere che i primi rilievi effettuati dalle forze di polizia possano essere alterati da criteri procedurali non conformi ai protocolli internazionali. L'operatore che giunge per primo sulla scena del crimine ha una responsabilità pari a quella di chi svolge le analisi successivamente. Ne consegue che il dato acquisito secondo modalità non conformi alle regole stabilite dai protocolli scientifici internazionali dev'essere considerato alterato e non dovrebbe poter essere utilizzato in giudizio. Infatti, il mancato rispetto degli standard operativi per la ricerca, acquisizione e conservazione dei campioni biologici grezzi può incidere notevolmente sull'attendibilità della successiva analisi degli stessi, inficiando così il regolare succedersi dei passaggi nel cd. "ciclo della prova biometrica"[346].

3.6.2. Il prelievo a scopi identificativi: la l. 85/2009 a più di dieci anni dalla sua entrata in vigore

Come già accennato in precedenza (cfr. il § 2), per l'analisi del Dna, potrebbe essere necessario prelevare campioni biologici direttamente dalla persona. Nell'ambito del prelievo coattivo finalizzato all'identificazione personale è intervenuta la nota legge 30.6.2009, n. 85, recante l'adesione al Trattato di Prüm sulla cooperazione transfrontaliera, diretto a contrastare il terrorismo, la criminalità

[342] Cfr. D.P.R. n. 87/2016 recante "*Disposizioni di attuazione della l. 30 giugno 2009, n. 85, concernente l'istituzione della banca dati nazionale del Dna e del laboratorio centrale per la banca dati nazionale del Dna*". Oltre a tale provvedimento, giova richiamare anche le "*Raccomandazioni Ge.FI nelle indagini di identificazione personale*" italiane e internazionali (I.S.F.G.) del 2018, aventi lo scopo di fornire uno strumento agli operatori di laboratorio nell'esecuzione e nella gestione di indagini genetico-forensi e nell'attuare gli opportuni controlli al fine di garantire un uso appropriato di indagini genetico-forensi sicure, efficaci ed affidabili e l'esecuzione di indagini genetico-forensi in laboratori con elevati standard di qualità.

[343] Ai fini dell'accreditamento, i laboratori devono elaborare un modello di lavoro descrivendolo in un apposito documento o procedura e applicandolo pedissequamente durante la conduzione delle analisi. C. Fanuele, *La prova del Dna*, cit., p. 598.

[344] Invero, esiste la possibilità che la ricerca all'interno della banca dati genetica nazionale individui una falsa corrispondenza a causa di errori nei laboratori di analisi del Dna oppure di inesatte registrazioni dei dati che possono provocare rilevanti conseguenze nel procedimento penale.

[345] Così, C. Fanuele, *La prova del DNA*, cit., p. 598, F. Fornari, *Epistemologia dell'errore giudiziario. Aspetti logici e casi pratici*, inAA.VV., *Genetica forense e diritto: prospettive scientifiche e processo penale ad un anno dalla legge*, (a cura di) M. Dobosz, E. Carnevali, M. Lancia, cit., pp. 887 e ss.

[346] In tal senso, cfr. C. Fanuele, *La prova del DNA*, cit., p. 599.

transnazionale e la migrazione straniera[347]. È fuori di dubbio che tale legge abbia realizzato - più o meno compiutamente[348] - un difficile contemperamento tra contrapposte garanzie costituzionali ed esigenze di repressione dei reati. Più nel dettaglio, al fine di rispettare l'art. 13 Cost. in materia di provvedimenti incidenti sulla libertà personale, con riferimento al prelievo coattivo di campioni biologici, è stata introdotta una disciplina piuttosto rigorosa che invidivua alcuni presupposti applicativi. Come noto, quando occorre eseguire dei prelievi di capelli, peli o mucosa boccale (mediante dunque un atto ripetibile), in mancanza del consenso del soggetto passivo e solo per i casi di urgenza, si è scelto di autorizzare il pubblico ministero a disporre tale atto nelle forme della consulenza tecnica *ex* art 359 *bis* c.p.p. In caso di mancata presentazione del soggetto interessato previamente avvertito, poi, l'autorità giudiziaria è legittimata a disporre l'accompagnamento e il prelievo coattivi, con decreto motivato in ordine alla sussistenza di esigenze investigative e ragioni di urgenza. Il provvedimento dev'essere poi convalidato nelle quarantotto ore successive decorrenti dalla sua esecuzione. Con riferimento, alle specifiche operazioni che possono essere compiute, il legislatore ha introdotto diversi rimedi senza però dettare una disciplina tassativa. In particolare, è stato previsto un doppio regime sanzionatorio della nullità, con riferimento alle operazioni, e dell'inutilizzabilità, riguardante le informazioni acquisite (v. 359 *bis* c.p.p.). Per vero, sussiste un mancato coordinamento tra l'art. 359 *bis* e l'art. 224 *bis* c.p.p., poiché sono previste sanzioni diverse per le medesime ipotesi. Mentre l'art. 224 *bis* comma 2 c.p.p. sanziona con la nullità l'ordinanza carente del contenuto previsto dalla legge, l'art. 359 *bis* prevede un'inutilizzabilità "speciale" in caso di violazione dei divieti fissati dall'art. 224 *bis* c.p.p. commi 4 e 5, ove peraltro non risultano specificate omologhe sanzioni espresse. Per l'esecuzione delle operazioni peritali, ai sensi dell'art. 224 *bis* co. 4 e 5, il giudice non può disporre attività contrastanti con specifici divieti di legge o tali da mettere in pericolo la vita, l'integrità fisica o la salute della persona o del nascituro, ovvero che, secondo la scienza medica possono provocare sofferenze di non lieve entità. Con riferimento all'esecuzione delle operazioni, le modalità devono rispettare la dignità e il pudore del destinatario dell'atto, parametri piuttosto vaghi rispetto ai quali calibrare il bilanciamento fra esigenze opposte.

Sebbene si ritenga che gli ambiti applicativi delle due disposizioni debbano rimanere ragionevolmente separati[349], sussiste poi una mancanza di coordinamento tra la disciplina contenuta

[347] Concluso il 27 maggio 2005 tra il Regno del Belgio, la Repubblica federale di Germania, il Regno di Spagna, la Repubblica francese, il Granducato di Lussemburgo, il Regno dei Paesi Bassi e la Repubblica d'Austria e relativo all'attuazione della cooperazione transfrontaliera, in particolare allo scopo di contrastare il terrorismo, la criminalità transfrontaliera e la migrazione illegale (Trattato di Prüm). Esso costituisce un esempio di cooperazione "rafforzata" realizzata esternamente alla cornice comunitaria. Successivamente con la decisione 2008/615/GAI il Trattato è stato incorporato nel quadro giuridico dell'Unione europea. Cfr. il capitolo II, § 1.5.1.2.

[348] Cfr. B. Lavarini, *Elementi di procedura penale*, cit., p. 95.

[349] Si esclude che i campioni biologici, prelevati ai fini dell'identificazione dell'indagato, possano essere utilizzati a fini probatori nel prosgieguo del procedimento e comparati eventualmente con le tracce organiche prelevate sulla scena del crimine.

nell'art. 224 *bis* e quella contenuta nell'art. 349, comma 2 *bis* c.p.p., riguardante l'oggetto del prelievo: da una parte capelli, peli o mucosa orale, dall'altra saliva o capelli (349 co. 2 *bis* c.p.p.)[350]. Sussiste ancora il dubbio ermeneutico relativo al carattere di tassatività o meno dell'elenco di atti richiamati dall'art. 224 *bis* co. 1 c.p.p., né appare sufficientemente determinata la seconda categoria di atti ("accertamenti medici") presi in considerazione dalla medesima norma (v. capitolo III, § 2.1.1)[351]. Ulteriore *quaestio* concerne la possibilità che il prelievo coattivo possa essere eseguito nei confronti di soggetti diversi dall'indagato o imputato. È stato rilevato che la sussistenza di una previsione legislativa *ad hoc* costituisca una «condizione imprescindibile di legittimità per una simile operazione»[352] in conformità a quanto stabilito dall'articolo 13 Cost.

In generale la legge n. 85/2009 ha avuto il merito di introdurre un primo strato di regole, colmando così una grave lacuna normativa nel codice di rito. Tuttavia, a distanza ormai di diversi anni dalla sua entrata in vigore, non sembrano ancora essere state risolte diverse problematiche applicative già a partire dalla primissima fase del prelievo di Dna. Nella prassi giudiziaria, gli organi inquirenti continuano a ricorrere ad espedienti tesi ad aggirare la disciplina normativa[353]. Allo stato attuale, infatti, pur potendosi eseguire, anche in assenza del consenso dell'interessato, prelievi e accertamenti finalizzati all'analisi di tracce biologiche, nel rispetto di presupposti e limiti fissati dall'art. 224 *bis* c.p.p., molte di queste operazioni vengono effettuate di nascosto dagli inquirenti (per es. offrendo all'indagato una sigaretta al fine di poter analizzare la saliva da lui lasciata). Con riferimento ai campioni biologici raccolti all'insaputa dell'interessato da parte degli organi inquirenti artatamente acquisiti, le operazioni sono da ricondurre ad una particolare modalità di acquisizione delle tracce biologiche, in grado di eludere la consapevolezza del soggetto di fornire parti di tessuti provenienti dal proprio corpo per finalità probatorie[354]. La soluzione che parte della dottrina ha già prefigurato, quanto meno per quanto riguarda l'analisi del Dna, consiste nell'interpretare gli artt. 359 *bis* e 224 *bis* c.p.p. nel senso che gli organi inquirenti prima debbano tentare di acquisire il campione biologico grezzo con il consenso, e poi eventualmente, procedere coattivamente[355]. La giurisprudenza, invece, afferma l'assoluta legittimità di queste operazioni in ragione del fatto che il materiale biologico «non

Diversamente, il rischio che si corre è quello di eludere la disciplina ben più garantista dettata dal legislatore attraverso gli artt. 224 *bis* e 359 *bis* c.p.p. Su questo punto cfr. B. Lavarini, *Elementi di procedura penale*, cit., p. 124.

[350] Cfr. C. Fanuele, *La prova del DNA*, cit., p. 609.

[351] Cfr. su questi, *ex multis*, C. Bonzano, *Gli accertamenti medici coattivi. Le galità e proporzionalità nel regime della prova*, Wolters Kluwer, Milano, 2017.

[352] Cfr. C. Fanuele, *La prova del DNA*, cit., p. 609.

[353] Sul punto, cfr. A. Camon, *La disciplina delle indagini genetiche*, in *Cass. pen*., 2014, p. 1437 e C. Fanuele, *La prova del DNA*, cit., p. 611.

[354] Per una ricostruzione del tema cfr. T. Alesci, *Il corpo umano fonte di prova*, cit., p. 165.

[355] Sul punto cfr. C. Fanuele, *La prova del DNA*, cit., p. 614.

fa più parte della persona medesima»[356]. Dal momento che la separazione del campione biologico dal soggetto non comporta alcun intervento manipolatorio, non vi sarebbe alcuna potenziale lesione della libertà del soggetto, costituendo formalmente la traccia una "*res derelicta*".

Ci si domanda a questo punto quando si raggiungerà una fase davvero compiuta di regolamentazione delle specifiche operazioni lungo l'intero "ciclo della prova biometrica" avente ad oggetto il Dna. Certamente, a distanza di poco più di dieci anni, sono ancora presenti diversi dubbi ermeneutici: l'auspicata prospettiva dell'introduzione di disposizioni normative, aventi ad oggetto altri metodi di riconoscimento biometrico di più recente diffusione nel contesto giudiziario e su cui l'ampiezza del dibattito scientifico non è nemmeno lontanamente paragonabile a quella del tratto in esame, non risulta delle più ottimistiche.

3.6.3. La banca nazionale del Dna e il laboratorio centrale

Come già ricordato *supra*, la legge n. 85 del 2009, nell'intento di adempiere ad un obbligo internazionale in materia di cooperazione giudiziaria, ha istituito la banca dati nazionale del Dna[357]. In seguito il d.P.R. 7.4.2016 n. 87, in attuazione del citato provvedimento normativo, ha introdotto numerose regole per la gestione, la tipizzazione e la conservazione dei campioni biologici nell'archivio genetico, al fine di tutelare sia l'attendibilità dei dati acquisiti sia la riservatezza dei soggetti a cui questi appartengono. Scopo della normativa è stato quindi quello di facilitare l'identificazione degli autori dei delitti nel rispetto delle garanzie fondamentali dell'individuo[358].

Secondo quanto stabilito dagli artt. 7 e 8 della l. 85/2009, la banca dati nazionale raccoglie i profili del Dna dei soggetti di cui all'art. 9, commi 1 e 2; i profili del Dna relativi a reperti biologici acquisiti nel corso di procedimenti penali; i profili del Dna di persone scomparse o loro consanguinei, di cadaveri e resti cadaverici non identificati. Al laboratorio centrale, invece, compete l'attività di tipizzazione del profilo del Dna[359] dei soggetti indicati nell'art. 9, commi 1 e 2 e la conservazione dei campioni biologici dai quali sono tipizzati i profili del Dna. I laboratori delle forze di polizia o di altre istituzioni ad elevata specializzazione hanno poi il compito di tipizzare i reperti biologici acquisiti nel

[356] Cass. pen., Sez. I, 15.12.2013, n. 48907 in *CED Cass* n. 258269.

[357] Più nel dettaglio, l'art. 5 della legge n. 85 del 2009 ha istituito la banca dati nazionale del Dna, presso il Ministero dell'Interno (Dipartimento di pubblica sicurezza), e quella del laboratorio centrale per la banca dati nazionale del Dna, presso il Ministero della giustizia (Dipartimento dell'amministrazione penitenziaria).

[358] L'art. 12 co. 2 l. 85/2009 stabilisce appunto che «l'accesso ai dati contenuti nella banca dati nazionale del Dna è consentito alla polizia giudiziaria e all'autorità giudiziaria esclusivamente per fini di identificazione personale, nonché per le finalità di collaborazione internazionale di polizia». A tal proposito, è stata introdotta un'adeguata tutela penale (art. 14) in termini di conservazione dei dati e predisposizione di opportune misure per evitare "fughe" di informazioni.

[359] Per "tipizzazione" s'intende «il complesso delle operazioni tecniche di laboratorio che conducono alla produzione del profilo del DNA». Cfr. l'art. 6, l. 85/2009.

corso delle indagini preliminari e mandarli alla banca dati per eseguire eventuali comparazioni (art. 10, l. 85/2009). Assolutamente condivisibile l'intenzione del legislatore di tenere separati i luoghi di raccolta e di confronto dei profili di Dna (banca dati nazionale) rispetto a quello di estrazione dei suddetti profili e di conservazione dei campioni biologici (laboratorio centrale).

Con riferimento all'esigenza di garantire l'attendibilità del confronto genetico, è stata predisposta una serie di regole per la raccolta, l'analisi e la conservazione dei campioni biologici tramite un'adeguata formazione del personale che effettua il prelievo[360]. Sono stati disciplinati anche i passaggi successivi eseguiti dal laboratorio tra cui la registrazione informatizzata del plico contenente i campioni, l'apertura del plico sigillato, la tipizzazione di un solo campione[361], la trasformazione del profilo genetico in modello elettronico (cd. *template*) e il suo inserimento nella banca dati[362]. L'obiettivo di fondo che accompagna tutto il testo del regolamento n. 87/2016 è stato l'automatizzazione massima dei meccanismi di estrazione e comparazione del Dna al fine di ridurre al minimo l'errore umano (art. 20, d.P.R. 87/2016)[363]. Tuttavia, come evidenziato *supra*[364], tutti i sistemi automatici (o semi-automatici) di riconoscimento biometrico presentano sempre una soglia di errore possibile. Il legislatore avrebbe dunque potuto specificare meglio i possibili rischi legati all'impiego del sistema, al fine di rendere più trasparente il funzionamento del meccanismo di comparazione[365].

---

[360] In particolare, è stato ritenuto necessario utilizzare contenitori separati ed etichettati, conservati a temperatura ambiente e inviati senza ritardo al laboratorio centrale in un plico sigillato antieffrazione.

[361] La tipizzazione avviene attraverso uno specifico procedimento ("LIMS", acronimo di *Laboratory Information Management System*) che assicura la tracciabilità delle operazioni effettuate dal personale addetto al laboratorio.

[362] Il profilo del Dna viene inserito nella banca dati tramite l'impiego del software CODIS (*Combined DNA Index System*, v. https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet) utilizzato dall'80% dei Paesi europei in possesso di una banca dati del Dna. L'inserimento dei profili genetici deve essere eseguito secondo la modalità del doppio cieco che riduce così il rischio di un errato inserimento del dato. Più nel dettaglio, l'operatore inserisce la prima volta il profilo del Dna che sarà reso non visibile dal software. A questo punto, lo stesso operatore inserirà per una seconda volta lo stesso profilo e il software confronterà i due dati, se i valori saranno identici allora il profilo verrà accettato dal sistema e potrà essere inserito nella banca dati. Cfr. R. Biondo, S. Barbato, *L'organizzazione e il funzionamento della banca dati nazionale del Dna*, in AA.VV., *La Banca dati italiana del Dna. Limiti e prospettive della genetica forense*, (a cura di) L. Scaffardi, Il Mulino, Bologna, 2019, p. 72. Il CODIS, attraverso la tipizzazione genetica di 13 marcatori (CSF1P0, FGA, TH01, TPOX, VWA, D3S1358, D5S818, D7S820, D8S1179, D13S317, D16S539, D18S51 e D21S11) consente di distinguere e identificare, su basi statistiche, ogni singolo individuo rispetto ad una popolazione di riferimento. Questi marcatori sono sparsi in diversi cromosomi permettendo l'assortimento indipendente degli alleli e semplificando il calcolo della valutazione statistica del profilo ottenuto. Per un approfondimento cfr. B. Budowle *et al*., *CODIS and PCR-Based Short Tandem Repeat Loci: Law Enforcement Tools*, in *Promega Corporation (ed) Genetic Identity Conference Proceedings of the Second European Symposium on Human Identification*, pp. 73-88, (Madison, WI).

[363] Sul punto cfr. U. Ricci, *Un lampo di consapevolezza nella normativa italiana: il DNA oltre la suggestione e il mito*, in *Diritto penale e processo*, 6/2016, pp. 751 e ss.

[364] Cfr. il § 2.5.

[365] Una volta inserito il profilo all'interno della banca dati, esso viene comparato automaticamente con tutti i profili del Dna esistenti per verificare se vi sia o meno coincidenza con un altro profilo presente. Cfr. R. Biondo, S. Barbato, *L'organizzazione e il funzionamento della banca dati nazionale del Dna*, cit. p. 73.

Il regolamento del 2016 ha poi previsto specificamente che il sistema automatizzato debba avere idonea documentazione IQ/OQ o equivalente o superiore che dimostri la corretta installazione e la funzionalità dello strumento secondo i requisiti richiesti (art. 20)[366].

Rispetto all'interpretazione del profilo genetico, al fine di garantire l'attendibilità del risultato, è stato previsto che la lettura e la successiva attribuzione sia effettuata o da due soggetti diversi oppure dalla medesima persona ma in due momenti diversi (art. 23 lett. *e*, d.P.R. 87/2016). Va ribadito che l'individuazione di una corrispondenza all'interno della banca dati potrebbe risultare sbagliata per diversi ordini di ragioni: a causa di errori nei laboratori di analisi del Dna (dovuti per esempio alla contaminazione dei reperti o a un'erronea manipolazione degli stessi in laboratorio), oppure errori evitabili seguendo pedissequamente il procedimento previsto per la comparazione, o ancora errori dettati da corrispondenze di profili genetici derivanti da pure coincidenze e in quest'ultimo caso, l'errore si riferisce ad un limite causato dal «potere discriminatorio del modello analitico applicato»[367]. Campioni e reperti biologici acquisiti durante il procedimento penale devono essere tipizzati da laboratori specializzati delle forze di polizia o di altre istituzioni mediante un sistema informatizzato e poi inviati senza ritardo alla banca dati del Dna (art. 6, co. 4, d.P.R. 87/2016)[368]. A tal proposito, si è introdotto un obbligo di conservazione dell'elettroferogramma utilizzato per l'estrapolazione del Dna da laboratori accreditati diversi da quelli di polizia e dal laboratorio centrale[369]. In questo modo, si consente alla difesa di esercitare, un seppur minimo, controllo postumo circa la correttezza dell'attività di tipizzazione precedentemente eseguita.

Con riferimento alla consultazione dei dati, l'art. 12 co. 2 l. 85 permette l'accesso alla banca dati nazionale e al laboratorio esclusivamente alla polizia giudiziaria e all'autorità giudiziaria[370]. Rimane

---

[366] "IQ" sta per "*installation qualification*" e la documentazione consente la verifica e il collaudo del corretto montaggio della strumentazione, della presenza e del corretto posizionamento dei diversi componenti, del collegamento alle fonti di energia etc.; "OQ", invece, sta per "*operational qualification*", la cui attestazione consente la verifica e il collaudo di tutte le operazioni (meccaniche, elettroniche, etc.) effettuate dalle strumentazioni.

[367] F. Taroni, J. Vuille, L. Luparia, *La prova del Dna nella pronuncia della Cassazione sul caso Amanda Knox e Raffaele Sollecito*, in *www.dirittopenalecontemporaneo.it*, fasc. 1/2016., pp. 155 e ss.

[368] Il sistema di informatizzazione genera automaticamente un codice che, in tal modo, non consente l'identificazione diretta del campione biologico (art. 6, co. 5, reg. att.).

[369] L'elettroferogramma è il risultato dell'analisi elettroforetica della sequenza di frammenti del Dna utilizzata per estrapolare il profilo del Dna.

[370] Più nel dettaglio, il sistema informatizzato è organizzato su due livelli: il primo è impiegato a fini investigativi in ambito nazionale; il secondo è utilizzato per finalità di collaborazione internazionale di polizia, in conformità alle decisioni 2008/615/GAI e 2008/616/GAI del 23 giugno 2008, nonché per scopi di attuazione degli accordi internazionali resi esecutivi (art. 3, co. 3, reg. att.). Con riferimento al primo, l'esito del raffronto deve essere comunicato telematicamente tramite il portale della banca dati ai laboratori delle forze di polizia che hanno inserito il profilo del Dna a fini comparativi. Si tratta di una sorta di accesso di secondo livello che permette di conoscere il nominativo associato al profilo genetico solo una volta che la comparazione sia risultata positiva. Rispetto al secondo, invece, per lo scambio dei dati provvede il Servizio per la cooperazione internazionale di polizia della Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza (art. 11, co. 1, reg. att.). Nell'ipotesi in cui la consultazione avvenga dall'estero verso l'Italia, essa è consentita nei punti di contatto esteri, in possesso delle credenziali

aperta la questione riguardo all'accesso nella banca dati da parte del difensore dell'indagato. In tal senso, si ritiene sarebbe stata auspicabile l'introduzione di un sistema di accesso anche al legale della persona direttamente interessata dal prelievo al fine di conoscere i risultati delle analisi e l'uso che ne poteva essere fatto.

Infine, occorre soffermarsi su alcune *quaestiones* circa la cancellazione dei dati e la distruzione dei campioni biologici. Innanzitutto giova evidenziare come il regolamento abbia introdotto alcuni aspetti innovativi rispetto alla normativa originaria[371]. Infatti, con riferimento alla conservazione dei profili del Dna di persone soggette a restrizione e dei relativi campioni biologici, è stato abbreviato il termine decorrente dalla data di registrazione: da quarant'anni a trenta (art. 25, co. 1). Il termine si estende a quarant'anni nei casi di particolare gravità del reato e di presunta pericolosità del condannato (art. 25, co. 2, reg. att.). Quanto alla conservazione dei campioni biologici, invece, l'art. 24 del regolamento ha previsto che il Dna estratto da questi sia distrutto successivamente al procedimento di tipizzazione. La parte di campione biologico grezzo non utilizzata deve essere conservata per otto anni[372]: una volta decorso questo lasso di tempo, il personale abilitato del laboratorio deve distruggere questi campioni, previa verbalizzazione delle operazioni. Il regolamento attuativo ha introdotto una serie di diritti per gli interessati finalizzati al controllo sull'uso dei propri dati personali. La normativa introdotta nel 2016, infatti, non mira solo a tutelare il diritto alla riservatezza, ma anche quello all'autodeterminazione informativa, ossia a conoscere, passaggio dopo passaggio, la destinazione delle proprie informazioni personali[373]. Al fine di tutelare la riservatezza del soggetto, di particolare importanza è stata poi la scelta effettuata dal legislatore di creare più banche dati, comprendenti informazioni distinte. La predisposizione di due archivi separati, uno contenente i dati genetici e l'altro le informazioni anagrafiche della singola persona, rende più difficili eventuali attacchi dall'esterno per impossessarsi di entrambe le specie di informazioni[374]. Oltre a questo è stata introdotta la

di autenticazione ed autorizzazione. Nel caso in cui la polizia giudiziaria debba ricercare un profilo del Dna in ambito internazionale, essa deve formulare una specifica richiesta al punto di contatto nazionale.
Rimane fermo che, al fine di tutelare l'attendibilità del dato genetico contenuto nella banca dati, siano inseriti al primo livello i profili del Dna «a partire da un numero di *loci* pari a sette»; mentre «solo i profili del DNA che hanno un numero di *loci* uguale o superiore a dieci sono inseriti al secondo livello» (art. 10, co. 4, reg. att.).

[371] Cfr. C. Fanuele, *La prova del DNA*, cit., p. 624.

[372] Parte della dottrina critica tale aspetto in quanto sarebbe stato meglio prevedere la conservazione per lo stesso periodo di tempo del modello elettronico in grado di riconoscere la persona, rispetto al campione biologico che invece permette anche di risalire alle origine etniche o di svelare malattie ereditarie, elementi quindi che possono originare svariate forme di discriminazione. C. Fanuele, *Dati genetici e procedimento penale*, cit., p. 326.

[373] L'art. 33 reg. att. conferisce al soggetto interessato il diritto di chiedere alla Direzione centrale della polizia criminale se nella banca dati del Dna esistono dati personali che li riguardano: una volta esperiti i necessari accertamenti, la Direzione sarà tenuta a rispondere entro trenta giorni. Quest'ultima potrà evitare di provvedere quando la richiesta potrebbe pregiudicare azioni o operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione della criminalità, dando senza ritardo informazione al Garante per la protezione dei dati personali.

[374] Cfr. C. Fanuele, *La prova del DNA*, cit., p. 629.

possibilità di risalire al responsabile della banca dati (Direttore del Servizio per il sistema informativo interforze della Direzione centrale della polizia criminale del Dipartimento di polizia scientifica) e del laboratorio centrale (Direttore dell'Ufficio del laboratorio centrale presso il Dipartimento dell'amministrazione penitenziaria).

Benché siano state introdotte disposizioni aventi un'indubbia portata garantista nei confronti dell'interessato, non è stata prevista alcuna disciplina per gli archivi e le banche dati appartenenti alle forze di polizia al fine di assicurare che non rimangano attive per attività differenti ovvero non duplichino i dati registrati una volta trasferiti i profili alla banca dati nazionale. Nonostante la sussistenza di problematiche poste in luce poc'anzi, si ritiene che la legge n. 85/2009 possa costituire - con le dovute cautele - un valido punto di partenza per la regolamentazione di altri sistemi di riconoscimento, seppur vi siano, come visto nei precedenti paragrafi, differenze ontologiche fra gli stessi. La "fortuna" della normativa in commento è stata proprio quella di essere espressione condivisa della maggior parte di scienziati e giuristi che, concordemente, si sono impegnati nella costruzione di una regolamentazione che tenesse in considerazione le principali questioni tecniche e scientifiche senza tralasciare fondamentali problematiche giuridiche.

4. Spunti di riflessione sulle banche dati tecnico-scientifiche a uso forense

Come visto poc'anzi, l'impiego del Dna a scopi identificativi, pur essendo stato regolamentato negli anni (pressoché) compiutamente dal legislatore[375], presenta ancora diversi profili problematici. Questi ultimi interessano in realtà tutte le categorie di dati biometrici il cui utilizzo risulta sempre più esteso. Accanto a lacune normative sullo sviluppo o progettazione di sistemi di raccolta e conservazione dei dati, si riscontrano, similmente a quanto detto per il Dna, problematiche relative alla tutela dei diritti del soggetto a cui tali dati personali appartengono, in particolare con riguardo al diritto alla riservatezza (cfr. *infra*, il capitolo III § 2.4). In generale, per i dati biometrici si registra un ampio dibattito dottrinario, politico, ma anche giurisprudenziale rispetto ai limiti e alla legittimità del loro impiego, raccolta, accesso e conservazione all'interno di ampie banche dati[376]. Contestualmente, per far fronte a problematiche di sicurezza e prevenzione dei crimini, le forze di polizia della maggior parte dei governi europei si stanno dotando di sistemi basati sulla raccolta di dati biometrici in grado di garantire un'accuratezza dell'identificazione molto elevata (96,5% per le impronte e 99,5% per l'iride). Tali dati, come visto, non solo vengono raccolti al fine di autenticare ovvero identificare determinati soggetti, ma sono anche immagazzinati in database gestiti solitamente da autorità di

[375] Cfr. il § 3.6.2.

[376] Cfr. *ex multis* L. Scaffardi, *Dati genetici e biometrici: nuove frontiere per le attività investigative*, in AA.VV., *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, (a cura di) L. Scaffardi, Giappichelli, Torino, 2018, pp. 37-64.

pubblica sicurezza. Queste ultime, attingendo ai dati contenuti e conservati nel database centrale, effettuano operazioni di *match* tra le informazioni inviate e quelle in loro possesso, al fine di determinare e verificare con sicurezza l'identità del soggetto. La problematica principale di questi sistemi strutturati - in diversi passaggi e controlli - risiede, per lo più, nella mancanza di una copertura normativa primaria apposita e nella difficoltà di inquadrare gli stessi entro i tradizionali istituti previsti dalla legge. Più nel dettaglio, si evidenzia una vistosa lacuna rispetto ai meccanismi di controllo nel trattamento e nella gestione dei dati biometrici digitalizzati rispetto all'intero "ciclo biometrico". A tal proposito, la direttiva 2016/680/UE, ai sensi dell'art. 41, regola la designazione e l'esercizio della funzione di controllo da parte di un'autorità indipendente. Ma fino a che punto questo può essere concretamente attuato nella prassi? L'impiego sistematico di software a fini di riconoscimento può dirsi oggetto di una verifica costante da parte di un'autorità di controllo? Il dubbio sorge dal momento che i passaggi tecnici per la gestione e la trasformazione di una traccia in dato biometrico digitalizzato sono molteplici ma non sempre così chiari al legislatore.

Come si può ben comprendere da questa breve ricostruzione, le problematiche più diffuse sorgono non solo con riferimento alla tutela della protezione dei dati, vista la particolare invasività che il possesso di tutte queste informazioni comporta nella sfera privata. Il timore sotteso a sistemi di raccolta massiva, conservazione e trattamento dei dati biometrici, così privi di idonea regolamentazione, riguarda essenzialmente il rischio di una vera e propria *mass surveillance* da parte dello Stato a fini di prevenzione. Di fondamentale importanza diventa la verifica della determinazione di limiti e garanzie in grado di stabilire un corretto bilanciamento tra i diversi interessi e diritti in gioco: da un lato la libertà personale, la libertà di manifestazione del pensiero, la dignità umana e la tutela alla riservatezza, dall'altro la sicurezza pubblica (cfr. il capitolo III, §§ 2 e ss. e il capitolo IV, §§ 3 e ss.). Ecco che, sotto questo profilo, risulta evidente come le complesse questioni giuridiche affrontate ed enucleate con riferimento ai dati genetici possano ragionevolmente porsi anche in relazione ai dati biometrici *tout court*, raccolti per scopi differenti da quelli investigativi (per esempio autenticativi) e conservati in un database centrale a cui però, in presenza di determinate condizioni, le autorità pubbliche possono avere accesso. Parte della dottrina ha già posto in luce come i concetti di «prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali» che "giustificano" l'accesso da parte delle autorità di *law enforcement*, in conformità a quanto stabilito dall'art. 1 d.lgs. 18.5.2018 n. 51[377], siano ancora troppo vaghi e privi di idonee tutele dei soggetti interessati. Ne consegue che, a fronte di una lampante lacuna normativa rispetto alla maggior parte

[377] Cfr. *supra* il § 1.1. Il d.lgs. ha attuato la direttiva 2016/680/UE del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla 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, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU Serie Generale n.119 del 24.5.2018).

dei sistemi di riconoscimento biometrici presenti nel territorio nazionale, i database di dati biometrici utilizzati a scopo autenticativo o di categorizzazione sollevano problematiche giuridiche sotto il profilo della riservatezza e della protezione dei dati nonché complesse e delicate questioni di legittimità costituzionale. In generale, per quanto i sistemi di autenticazione basati su modelli biometrici siano interessanti sotto diversi punti di vista[378], necessitano di essere supportati da apparati normativi di forte tutela della riservatezza, al fine di scongiurare il pericolo di sorveglianza di massa o di sfruttamento dei dati da parte non solo dello Stato, ma anche di soggetti privati e, per quanto qui interessa, laddove l'accesso e l'uso venga effettuato da autorità pubbliche per finalità di tutela della sicurezza o repressione dei crimini. La banca dati nazionale del Dna rappresenta un interessante spunto di riflessione che induce a interrogarsi sui limiti che devono essere posti alla raccolta e conservazione di dati così personali quali quelli biometrici in apposite banche dati. Queste presentano dei rischi intrinseci rappresentati dalla possibilità di giungere a forme di controllo "generalizzate" della popolazione, finanche ad una vera e propria attività di profilazione. Ne consegue che il rischio più elevato, nel caso di utilizzo dei dati biometrici, non sia rappresentato tanto dall'integrazione all'interno di carte d'identità o passaporti di tali tipologie particolari di dati, quanto dalla creazione di database. È forte la sensazione di trovarsi di fronte ad una "nuova stagione del costituzionalismo", caratterizzata da un emergente potere sovrano. In altre parole, sta emergendo sempre di più un «paradigma tecnologico che si presenta come dominante, come fattore di liberazione della persona e di innovazione irresistibile, dunque irrinunciabile»[379].

La riflessione conclusiva di questo primo capitolo non può che partire da tale elemento, al fine di sviluppare un pensiero critico positivo, evitando l'immobile prospettiva di chi vorrebbe un impossibile ritorno al passato. È necessario invece un approccio multidisciplinare e di "coesistenza" tra scienza e diritto. Un diritto "nuovo" che sia in grado di regolamentare discipline che attengono sempre di più ai diritti e ai connessi strumenti di tutela volti a limitare il più possibile quei nocivi effetti discriminatori su beni fondamentali che spaziano dalla dignità all'identità personale. Oltre a questo, con riferimento a determinati dati biometrici[380], non è più sufficiente tenere in conto i soli diritti legati all'identità individuale, ma si devono considerare anche quelli che coinvolgono tutti i membri di quel nucleo aperto e complesso rappresentato da coloro che condividono la stessa linea ereditaria[381]. Ne deriva un

[378] Gli usi indiretti di archivi creati con scopi autenticativi sono essenzialmente legati alla sicurezza, prevenzione e repressione dei reati.

[379] Cfr. A. Simoncini, *Sovranità e potere nell'era digitale*, in AA.VV., *Diritti e libertà in internet*, (a cura di) O. Pollicino, T.E. Frosini, E. Apa, Mondadori, Milano, 2017, p. 20.

[380] Piuttosto lampante è il caso del Dna.

[381] «Le informazioni genetiche, infatti, sebbene costituiscano il nucleo più profondo dell'identità di un soggetto ed, in tal senso, lo rendono unico e lo distinguono da chiunque altro, tuttavia rappresentano al contempo un ponte tra le diverse generazioni umane e così i dati riferibili ad una singola persona "raccontano" indirettamente la storia biologica di tutti gli appartenenti al medesimo

concetto piuttosto inedito di "parentela biometrica" che può ricomprendere così l'intero gruppo biologico che condivide parte di questo patrimonio. In tal senso, l'inserimento di un membro della famiglia all'interno della banca dati potrebbe far venir meno il diritto alla riservatezza dell'intero gruppo, portando alla luce, in caso di indagini specifiche, vincoli di sangue non prevedibili[382].

Un ulteriore profilo di riflessione attiene al fatto che talune ricerche "randomiche" all'interno di banche dati prive di un'uniforme regolamentazione vanno a porre nel database, cui la polizia può accedere, un novero di soggetti che vengono privati di alcune delle garanzie tipiche e delle procedure previste dalla legge, come quella sulle acquisizioni coattive dei campioni biologici grezzi ovvero sulla cancellazione del dato. Tutto ciò spinge a intendere il fenomeno come uno *screening* silente, che è stato definito da alcuni come il «*lifetime of genetic surveillance*»[383], in grado di sottoporre sistematicamente la popolazione a prelievi di dati biometrici, senza alcuna formale regolamentazione.

Come si avrà modo di approfondire nei prossimi capitoli, l'uso dei dati biometrici fa sorgere numerose e ulteriori questioni giuridiche, attinenti non solo alla conservazione e all'accesso a tali informazioni ma anche all'adeguatezza o meno dell'attuale disciplina esistente in ambito nazionale. Compito del legislatore è quello di predisporre discipline normative capaci di regolare compiutamente l'uso di questi fondamentali dati personali, garantendo un corretto e proporzionato bilanciamento tra gli innegabili vantaggi derivanti dal loro utilizzo e i rischi di un'eccessiva compressione dei diritti fondamentali dell'individuo.

È tempo che questo preannunciato intreccio di limiti e opportunità sia sciolto. Un decisivo punto di partenza a favore dell'utilizzo di dati contenuti in questi archivi automatizzati deve essere un necessario diritto di accesso e di controllo da parte dei soggetti interessati, funzionale alla verifica sulla rilevanza, necessità e proporzionalità dell'impiego dei dati stessi, senza che questi possano essere utilizzati in modo randomico.

---

ambito famigliare o gruppo biologico». Cfr. V. D'Antonio, *I dati genetici*, in AA.VV., *Il codice dei dati personali. Temi e problemi*, (a cura di) F. Cardarelli, S. Sica, V. Z. Zencovich, Giuffrè Editore, Milano, 2004, p. 351.

[382] «La imprevedibile combinazione tra diritto e scienza può portare a sovvertire vite, a scompigliare equilibri familiari consolidati, a rivelare segreti mai confessati e che appartengono alla sfera doverosamente riservata di ciascun individuo». Cfr. G. Gennari, *La istituzione della Banca dati del DNA ad uso forense: dalla privacy alla sicurezza*, in AA.VV., *Prelievo del DNA e banca dati nazionale*, (a cura di) A. Scarcella, Cedam, Padova, 2009, p. 75.

[383] Cfr. D.E. Roberts, *Collateral Consequences, Genetic Surveillance, and the New Biopolitics of Race*, University of Pennsylvania Law School, Pennysylvania, 2011, p. 582, ove l'autrice si spinge anche oltre questo concetto, affermando, sulla base dell'esperienza inglese e americana, come questo tipo di attività possa portare alla correlazione tra determinati fenomeni criminali e appartenenze etniche, foriere di politiche discriminatorie.

CAPITOLO II

GLI ALGORITMI DELL'IDENTITA': "CORPO ELETTRONICO" E *DIGITAL EVIDENCE* A CONFRONTO[*]

«*Aspetto con impazienza il giorno in cui il processo penale consisterà nel sedersi a guardare la verità digitale*»[1].

J. FRANZEN

SOMMARIO: - 1. "Macchine come me": analisi ontologico-giuridica della rappresentazione digitale del tratto biometrico e del *template*. - 1.1. Le principali caratteristiche della prova digitale (immaterialità, dispersione, promiscuità, ubiquità, modificabilità). - 1.2. La *digital evidence* e la sua efficacia probatoria: l'individuazione, l'acquisizione, la conservazione, l'analisi e la presentazione. - 1.3. La *Digital Forensics* in Italia: aspetti normativi. Le norme del codice di procedura penale introdotte con l. 18.3.2008, n. 48. - 1.3.1. Sulla ripetibilità o irripetibilità delle operazioni: dalla *digital evidence*… - 1.3.2. …alla *digital proof*. - 1.4. Le intercettazioni: quello che le norme (ancora) non dicono. - 1.4.1. Il riconoscimento informale della voce ad opera della polizia giudiziaria. - 1.4.2. La modalità *real time* dei software di riconoscimento facciale. - 1.5. Cenni sulla cooperazione giudiziaria internazionale per la raccolta e acquisizione dei modelli elettronici. - 1.5.1. (segue) i diversi strumenti normativi. - 1.5.1.1. La direttiva 2016/680/UE. - 1.5.1.2. Il Trattato di Prüm e le decisioni 2008/615/GAI e 2008/616/GAI. - 1.5.1.2. Cenni sulla direttiva 2014/41/UE. - 1.5.1.3. La proposta di regolamento sugli ordini di produzione e conservazione di prove elettroniche 2018/0108 (COD). - 1.5.2. Le richieste di evidenze digitali ai *service providers* di Paesi extra UE. - 2. "*Automatedly generated evidence*" e tecniche di intelligenza artificiale: definizioni e ambiti applicativi. - 2.1. Il quadro normativo di riferimento: una ricostruzione dello stato dell'arte. - 2.1.1. La proposta di regolamento europeo sull'intelligenza artificiale 2021/0106(COD). - 2.2. I principi fondamentali in materia di intelligenza artificiale e giustizia alla luce del quadro giuridico attuale. - 3. Tecniche di intelligenza artificiale applicate alla disciplina biometrica. - 3.1. Sistemi di riconoscimento biometrico e normativa europea: un "percorso di conformità" alla proposta di regolamento. - 4. Alcune riflessioni conclusive.

[*] Il presente capitolo è costituito in parte dai seguenti contributi già pubblicati, E. Sacchetto, *Biometrics as forensic evidence: some reflections from the Italian Criminal proceeding's point of view*, in *8th International Workshop on Biometrics and Forensics (IWBF)*, 2020, E. Sacchetto, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *www.lalegislazionepenale.it*, 16.10.2020, E. Sacchetto, *Brevi riflessioni sui fondamenti e sui limiti del rapporto fra automated faced-based human recognition technology e processo penale*, in *ASTRID*, 2022 (in via di pubblicazione) e E. Sacchetto, *Automated faced-based human recognition technologies e procedimento penale alla luce della proposta di regolamento sull'IA: alcuni spunti di riflessione*, in AA.VV., *Collana del Centro Studi Giuridici del Dipartimento di Economia di Ca' Foscari*, (a cura di) C. Camardi, *atti del Convegno* **"***La via europea per l'intelligenza artificiale*", Venezia il 25-26.11.2022 (in via di pubblicazione).

[1] J. Franzen, *Purity*, Einaudi, Torino, 2016, p. 550.

1. "Macchine come me": analisi ontologico-giuridica della rappresentazione digitale del tratto biometrico e del *template* [2]

L'evoluzione della scienza e della tecnica ha avuto un'incidenza di fortissimo rilievo sul corpo del vivente[3]. Come già osservato nel capitolo I[4], il corpo umano è in grado di fornire molteplici informazioni utili all'accertamento del reato, anche a prescindere dall'atteggiamento partecipativo del suo titolare (cfr. *supra* il capitolo I, § 2). In tal senso, esso è stato definito un «oggetto giuridico nuovo» e «in continua trasformazione»[5]. Nel tempo, infatti, il corpo umano ha perso la sua connotazione unitaria scomponendosi in diverse parti, tra cui organi, tessuti e cellule, separabili dal corpo d'origine. Tale forma di "disarticolazione" ha raggiunto il suo ακμή nella fase in cui ad esso si è iniziato a contrapporre il corpo elettronico[6]. Più nel dettaglio, quest'ultimo ha assunto una particolare importanza allorquando i dati biometrici digitalizzati si sono rivelati uno strumento irrinunciabile per l'attribuzione e il riconoscimento dell'identità, posta - talvolta - l'inadeguatezza dei campioni grezzi ad assicurare da soli la certezza dell'identificazione o dell'autenticazione del soggetto[7]. In tal guisa, si è tornati a dare rilievo, in una modalità del tutto inedita, al corpo, che è diventato fonte di altre informazioni, oggetto di un continuo «*data mining*» da cui attingere ulteriori dati fondamentali[8]. Il

[2] Il titolo del paragrafo è ispirato al romanzo di I. McEwan, *Macchine come me*, Einaudi, Torino, 2019.

[3] In questo senso, cfr. T. Alesci, *Il corpo umano come fonte di prova*, Wolters Kluwer, Milano, 2017, p. 57 e F. Siracusano, *La prova informatica*, Associazione tra gli studiosi del processo penale "G.D. Pisapia", XXX Convegno Nazionale, Roma 20-21 ottobre 2016 – Università La Sapienza "*Investigazioni e prove transnazionali*".

[4] Cfr. il capitolo I, § 2.

[5] Cfr. S. Rodotà, *Ipotesi sul corpo "giuridificato*", in S. Rodotà, *Tecnologie e diritti*, (a cura di) G. Alpa, M. R. Marella, G. Marini, Bologna, 1995, p. 204. Nello stesso senso cfr. T. Alesci, *Il corpo umano come fonte di prova*, cit., p. 57.

[6] Cfr. T. Alesci, *Il corpo umano come fonte di prova*, cit., p. 57 e F. Siracusano, *La prova informatica*, cit., p. 1, a proposito dei dispositivi informatici afferma che «il bagaglio di informazioni in essi contenuto costituisce una sorta di "corpo elettronico" – *pendant* del "corpo fisico" di ogni individuo – che ormai ciascuno di noi possiede e che lascia tracce ovunque. Un "corpo elettronico" dotato di sconfinata capienza, idoneo ad accogliere una massa sterminata d'informazioni capaci di rilevare il contenuto d'intere esistenze e adatte a sedare anche la più bulimica istanza di conoscenza. Un corpo, tra l'altro, *light*: facile da trasportare; rapido nei suoi spostamenti sì da renderlo, spesso, delocalizzabile. Un corpo, comunque, da tutelare e rispetto al quale le tradizionali garanzie apprestate per porre al riparo l'individuo da indesiderate invasioni della propria sfera personale si mostrano spesso inadeguate». Alla distinzione fra "corpo fisico" e "corpo elettronico" fa cenno anche C. Cajani, *Le richieste per finalità di giustizia rivolte agli Internet service providers esteri*, in AA.VV., *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, (a cura di) S. Aterno, F. Cajani, G. Costabile, D. Curtotti, Giappichelli, Torino, 2021, p. 410 e P.G. Monateri, *Diritti senza tempo né spazio*, in *Sole24ore*, 23.12.2012, p. 33. Di "corpo elettronico" parla anche L. Parlato, *Libertà della persona nell'uso delle tecnologie digitali*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*, (a cura di) L. Kalb, Giuffrè, Milano, 2019, p. 211. E. Mordini, *Il Volto e il Nome. Implicazioni Etiche, Sociali e Antropologiche delle Tecniche di Identificazione Biometriche, MEDIC*, 2006, 14, p. 40, parla, invece, di "corpo digitale" come «un corpo disperso, contenuto nei mille rivoli elettronici della rete; per un altro verso è invece un corpo quanto mai compatto».

[7] Stefano Rodotà è stato uno dei primi studiosi a evidenziare la necessità di un ricorso sempre più frequente ai dati biometrici digitalizzati. V. S. Rodotà, *Trasformazioni del corpo*, in *Pol. dir*., 2006, 3.

[8] «(…) dalla *Società Disciplinare* di Focault, in cui l'individuo è osservato dal guardiano nella torre, si è passati al controllo della persona tramutata in *alter-ego* virtuale digitale, in dati sensibili, linfa vitale della società dell'informazione: è il database, tesoro inestimabile dei tempi moderni, la chiave di vigilanza sull'individuo», cfr. G. Cecanese, *Le pre-investigazioni informatiche e i controlli sui* social, in AA.VV., *Le pre-investigazioni. Espedienti e mezzi*, (a cura di) A. Scalfati, Giappichelli, Torino, 2020, p. 268. Anche U. Pagallo, *Introduzione alla fisolofia digitale. Da Leibniz a Chaitin*, Giappichelli, Torino, 2005, pp. 1-8 sottolinea

corpo è divenuto una vera e propria *password*: i modelli elettronici delle impronte digitali, della geometria della mano, dell'iride, della retina, dei tratti del volto, della voce, della firma, del Dna e dell'andatura hanno di fatto preso il posto di parole chiave astratte[9].

Gli stessi dispositivi IoT[10] hanno iniziato col tempo a fornire evidenze che riguardano dati personali e, in alcuni casi, funzioni vitali del nostro corpo: dal battito cardiaco, alla pressione arteriosa, al numero di passi compiuti, fino alle abitudini alimentari[11]. Gli *smartphone* di ultima generazione

---

che i dati digitali costituiscono un aspetto fondamentale della società moderna. Su questo punto cfr. J. Nieva-Fenoll, *Intelligenza artificiale e processo*, cit., p. 15. S. Quattrocolo, *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Rev. Italo-espanola derecho procesal*, 2018, 2, p. 111, afferma come «la raccolta (attraverso la captazione occulta, ma non solo) di dati relativi alla sfera individuale dell'indagato garantisce sempre di più la ricostruzione di abitudini, di interessi, inclinazioni, stili di vita che possono rappresentare un corollario indiziario estremamente importante ai fini processuali». Per "*data mining*" s'intende il procedimento logico con cui programmi automatici o semi-automatici estraggono informazioni da grandi quantità di dati. Cfr. *ex multis* G. Oatley, B. Ewart, *Data mining and crime analysis*, in *Wiley Interdisciplinary Reviews (WIREs): Data Minining and Knowledge Discovery* 1(2), pp. 147–153. S. Smyth, *Biometrics, surveillance and the law. Societies of restricted access, discipline and control*, Routledge, New York, p. 70 si preoccupa del fatto che «*the system runs it through a facial recognition system and your name, age, social media profile and criminal record pops up – your whole identity is revealed from a single source of biometric data – your face*».

[9] Cfr. sul punto T. Alesci, *Il corpo umano fonte di prova*, Cedam, Milano, p. 59 e S. Smyth, *Biometrics, surveillance and the law. Societies of restricted access, discipline and control*, cit., pp. 1 e ss.
Giova ricordare che nel capitolo II si intende ricondurre la rappresentazione digitale del dato biometrico e il *template* entro alcune delle categorie dogmatiche processuali tradizionali, fornendo al lettore alcuni parametri che saranno utili per l'analisi del "corpo elettronico" nello spettro delle garanzie processuali fondamentali (v. il capitolo III).

[10] Definito come «una rete mondiale di oggetti interconnessi univocamente indirizzabili, basata su protocolli di comunicazione standard». D. Bandyopadhyay, J. Sen, *Internet of Things: Applications and Challenges in Technology and Standardization*, in *Wirel. Pers. Commun.*, vol. 58, no. 1, pp. 49-69, 2011. Con la locuzione *Information Technology* ci si riferisce dunque all'impiego di sistemi digitali per memorizzare, modificare e recuperare i dati. *Internet of things* è stato definito anche come «un'estensione di internet al mondo degli oggetti e dei luoghi concreti, cioè far sì che il mondo elettronico tracci una mappa di quello reale, dando una identità elettronica, un identificativo unico alle cose e ai luoghi dell'ambiente fisico». Insomma costituisce «una infrastruttura di rete dinamica e globale dove "oggetti" fisici e virtuali sono dotati di una propria identità, di attributi fisici e di interfacce intelligenti». G. Costabile, *Digital forensics & digital investigation: classificazione, tecniche e linee guida nazionali ed internazionali*, in AA.VV., *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, (a cura di) S. Aterno, F. Cajani, G. Costabile, D. Curtotti, Giappichelli, Torino, 2021, p. 26. Quando le tecnologie informatiche sono impiegate nell'ambito delle telecomunicazioni l'IT prende il nome di *Information and Communication Technology*, ovvero di tecnologie dell'informazione e della comunicazione. Cfr. S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 10. Sulla diffusione dell'IoT, cfr. P. G. Bizzarro, *Il futuro è nei dati: data sharing e data spaces nel mercato unico europeo*, disponibile su https://datavalley.it/2021/04/07/il-futuro-e-nei-dati-data-sharing-e-data-spaces-nel-mercato-unico europeo/?fbclid=IwAR3ofkdNg5hQzJeQyMjhYigAqfn0I6vHbH21-pxAFa7i8JgALELpFdRlEbw (ultimo accesso il 12.4.2021) e F. Nicolicchia, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Wolter Kluwer, Milano, 2020, pp. 4 e ss.

[11] La Corte Suprema degli Stati Uniti d'America, in *Riley v. California, 573 U.S. (2014)*, ha affermato che «*these cases require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy*», v. G. Lasagni, *Tackling phone searches in Italy and the United States: Proposals for a technological rethinking of procedural rights and freedoms*, in *New Journal of European Criminal Law*, 2018, pp. 383– 401, p. 391. Sul punto cfr. anche Colarocco, T. Grotto, G. Vaciago, *La prova digitale. La casistica civile e penale e gli strumenti di acquisizione in ambito cloud*, Giuffrè, Milano, 2020, p. 7, V.D. Lyon, *Massima sicurezza. Sorveglianza e "guerra al terrorismo"*, Cortina Raffaello, Milano, 2005, pp. 61-93, L. Luparia, *Computer crimes e procedimento penale*, in AA.VV., *Trattato di procedura penale*, (diretto da) G. Spangher, *Modelli differenziati di accertamento*, (a cura di) G. Garuti, Utet giuridica, Torino, 2011, pp. 374 e ss., M. Daniele, *La prova digitale nel processo penale*, in *Riv. dir. proc*., 2011, 283 e F. Palmiotto, *Le indagini informatiche e la tutela della riservatezza informatica*, in *www.lalegislazionepenale.it*, 1.7.2019, p. 6, in cui l'Autrice afferma espressamente che «l'individuo, mediante l'utilizzo di

presentano modalità di sbloccamento tramite sistemi di riconoscimento facciale[12]: questi ultimi vengono integrati nei *social media* per ottenere più visibilità e allargare il proprio *network* di conoscenze[13] e nelle *consolle* per creare esperienze più interattive[14]. Più di recente, durante l'emergenza pandemica da Covid-19, sono stati impiegati sistemi di riconoscimento facciale per monitorare gli studenti per gli esami a distanza[15], oppure per misurare la temperatura delle persone tra la folla, riconoscere soggetti tra coloro che non indossano la mascherina e tracciare potenziali infetti[16]. L'ampio utilizzo da parte della popolazione di sistemi di intelligenza artificiale[17], incorporati in dispositivi digitali, ha generato una varietà di dati del tutto inedita che può avere un impatto decisivo per l'andamento delle indagini e per l'accertamento[18]. Infatti, da un lato, gli strumenti informatici sono mezzo per la commissione di particolari reati e, dall'altro, le memorie dei dispositivi costituiscono altrettanti archivi di informazioni di cui gli organi inquirenti non possono più fare a meno per la ricostruzione del fatto[19].

Un dato biometrico può quindi trovarsi sottoforma di rappresentazione digitale del tratto ovvero di *template*, frutto di determinati procedimenti regolamentati di digitalizzazione a partire da un campione biometrico grezzo[20], può essere ricavato da un'immagine o da un video trattati tramite un "dispositivo

---

dispositivi elettronici, dallo *smartphone* al computer, crea uno spazio virtuale, immagazzinando una mole sempre più ingente di dati, informazioni e programmi che identificano un'entità complessa».

[12] Cfr. https://support.apple.com/it-it/HT208108 (visualizzato in data 21.5.2021).

[13] Cfr. https://forbes.it/2020/02/18/social-media-octi-riconoscimento-facciale-ar-realta-aumentata/ (visualizzato in data 21.5.2021).

[14] Cfr. https://www.playstationzone.it/news-ps-vita/video-riconoscimento-facciale-per-ps-vita/ (visualizzato in data 21.5.2021).

[15] Cfr. A. Dini, *La tecnologia per combattere imbrogli e distrazioni negli esami online*, in *La Stampa*, 12.5.2020, reperibile all'indirizzo https://www.lastampa.it/topnews/tempi-moderni/2020/05/12/news/la-tecnologia-per-combattere-imbrogli-e-distrazioni-negli-esami-online-1.38835127 (visualizzato in data 20.5.2021).

[16] Cfr. M. Van Natta et al., *The rise and regulation of thermal facial recognition technology during the Covid-19 pandemic*, in *Journal of Law and the Biosciences*, 7, 1, 2020.

[17] Sulla nozione di "intelligenza artificiale" si tornerà meglio *infra*, cfr. i §§ 2 e ss. Questa rapida diffusione si deve al «*rapid development of four self-reinforcing trends: even more sophisticated statistical and probabilistic methods; the availability of increasingly large amounts of data; the accessibility of cheap, enormous computational power; and the transformation of ever more places into IT-friendly environments (e.g. domotics and smart cities)*». C. Cath, S. Wachter. B. Mittelstadt, M. Taddeo, L. Floridi, *Artificial Intelligence and the 'Good Society': the US, EU, and UK approach*, in *Science and Eng. Ethics*, 2018, p. 505. La letteratura in argomento è assai ampia, cfr. *ex multis*, J. Kaplan, *Intelligenza artificiale. Guida al futuro prossimo*, Luiss, Roma, 2017, S. Hénin, *AI. Intelligenza artificiale tra incubo e sogno*, Hoepli, Milano, 2019, pp. 75 e ss. e AA.VV., *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations*, (a cura di) M. Caianiello, A. Camon, Wolters Kluwer, Milano, 2021, pp. 1 e ss.

[18] Cfr. sul punto U. Pagallo, S. Quattrocolo, *Fair Trial and the Equality of Arms in an Algorithmic Society*, in AA.VV., *Global Law. Legal Answers for Concrete Challenges*, (a cura di) M.L. Labate Mantovanini Padua Lima, J. Garcez Ghirardi, Juruà Editorial, Porto, 2018, pp. 261 e ss., S. Conti, *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, pp. 153-164.

[19] Cfr. G. Cecanese, *Le pre-investigazioni informatiche e i controlli sui social, cit*., p. 272, T. Huang, Z. Xiong Z. Zhange, *Face Recognition Applications*, in AA.VV., *The Handbook of Face Recognition*, (a cura di) Z.S. Li, A.K. Jain, Springer, New York, pp. 617 e ss.

[20] Nella classificazione operata da F. Palmiotto, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in AA.VV., *Algorithmic Governance and Governance of Algorithms, Legal and Ethical Challenges*, (a cura di) M. Ebers, M. Cantero Gamito, Springer, Berlin, 2020, p. 52, corrisponde alla "*computer generated evidence*".

tecnico specifico" ritraente un determinato dato biometrico (cfr. il capitolo I, § 2)[21], ovvero possono derivare direttamente da dati elaborati per un uso generico o commerciale[22], quindi estraneo al procedimento penale, quali assistenti domestici o dispositivi elettronici di rilevamento delle proprie caratteristiche fisiologiche o comportamentali. Volendo momentaneamente accantonare questi ultimi, perché non specificamente disciplinati dalla legge e non basati su protocolli sicuri[23], si ritiene che la prima tipologia, date le sue caratteristiche ontologiche, possa essere - seppur cautamente - ragionevolmente ricondotta entro la più ampia definizione di *digital evidence*[24]. Rispetto a tale

[21] «*Facial recognition on smartphones represents another important step in the evolution of high-tech policing. Beginning in 2010, dozens of law enforcement agencies in the United States were outfitted with a handheld facial recognition device known as MORIS, or Mobile Offender Recognition System, which attaches to an Apple iPhone, enabling an officer to snap a picture of a face from up to five feet away, or scan a person's irises from up to sixes inches away, and do an immediate search to see if there is a match with a criminal database*» S. Smyth, *Biometrics, surveillance and the law. Societies of restricted access, discipline and control*, Routledge, New York, pp. 67 e ss. Per esempio i risultati di un esame antropometrico effettuato attraverso un apposito software sulle immagini riprese da una telecamera che consistono in dati numerici e corrispondono alle misure di certe parti del corpo della persona ritratta. Per produrre tali dati l'esperto utilizza appositi dispositivi in conformità a ben precisi principi tecnici, i quali indicano le condizioni operative che garantiscono che i dati prodotti corrispondano alla realtà. Infatti, si ricorda che conformemente al considerando n. 51 del Regolamento (UE) 2016/679 (noto come GDPR ossia *General data protection regulation*), la semplice fotografia ritraente, per esempio, un volto non rientrerebbe nella macro categoria dei "dati biometrici", salvo quando l'immagine sia trattata attraverso un dispositivo tecnico specifico che consenta l'identificazione univoca o l'autenticazione di una persona fisica. Cfr. nello stesso senso anche il considerando n. 29 del Regolamento (UE) 2018/1725 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE. Cfr. https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018.pdf/1bd9bde0-d074-4ca8-b37d-82a3478fd5d3?version=1.9 e https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018R1725&from=IT (visualizzato in data 10.5.2021). Sul punto cfr. G. Carlizzi, *La valutazione della prova scientifica*, Giuffrè, Milano, 2019, pp. 14-17, M. H. Lim, A. B. J. Teoh, *Biometric Template Binarization*, in AA.VV., *Encyclopedia of Biometrics*, (a cura di) S. Z. Li, A. K. Jain, Springer, Boston, 2015, M. M. Plesnicar, A. Završnik, P. Šarf, *Fighiting Impunity with New Tools: How Big Data, Algorithms, Machine Learning and AI Shape the New Era of Criminal Justice*, in AA.VV., *The Fight Against Impunity in EU Law*, (a cura di) L. Marin, S. Montaldo, Hart Publishing, New York, 2020, p. 261, sostengono che «*in the near future, further steps along the line of the corporal importance of one's body for crime control are reasonably to be expected: from analysis of walking patterns, posture and face recognition for identification purposes (eg Facebook's DeepFace program) to analysis of facial expressions for emotion recognition*». Anche in questo caso il *template* potrebbe accostarsi alla categoria "*computer derived evidence*". Cfr. F. Palmiotto, *The Black Box on Trial*, cit. p. 52.

[22] «*The mobile app, paired with a compact fingerprint scanner device matches prints against two national databases of known images in less than a minute, and can thus also help officers identify individuals in emergency situations, and contact next of kin*» S. Smyth, *Biometrics, surveillance and the law. Societies of restricted access, discipline and control*, cit., p. 65. Cfr. l'efficace distinzione fra "prova digitale" e "*automatedly generated evidence*" operata da S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, p. 73. Per un approfondimento sulla prova generata automaticamente v. anche S. Quattrocolo, Processo penale e rivoluzione digitale: da ossimoro a endiadi? In *MediaLaws*, p. 121 e ss., S. Quattrocolo, *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Rev. Italo-espanola derecho procesal*, 2018, 2, pp. 107 e ss. Nella classificazione operata da F. Palmiotto, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, cit., p. 52 sarebbe la "*computer derived evidence*".

[23] Cfr. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, cit., p. 74.

[24] Si concorda con M. Pittiruti, *Digital evidence e procedimento penale*, Giappichelli, Torino, 2017, p. 8, che evidenzia come «ben può utilizzarsi la formula "*digital evidence*" quale recipiente ove includere ogni forma di utilizzo a fini procedimentali, in senso lato, di dati originariamente contenuti in supporti informatici o telematici, oppure ancora trasmessi in modalità digitale. A patto, però, di tenere a mente che si tratta di un fenomeno con diverse sfaccettature, che mal si presta a inquadramenti a priori ed è difficilmente conciliabile con le tradizionali distinzioni in tema di prova. Più in particolare, la natura multiforme del dato digitale

inquadramento concettuale, è bene però rimanere consapevoli dei «diversi livelli di complessità»[25] che pone il dato biometrico *tout court*, considerata l'intrinseca specificità delle fonti di prova in esame.

Dato biometrico digitalizzato:
a) *template* o rappresentazione digitalizzata del tratto (cfr. il capitolo I, § 2);
b) generato da un dispositivo di uso generico o commerciale;
c) ricavato dalla riproduzione digitalizzata di un dato biometrico trattato da un "dispositivo tecnico specifico" (per es. un volto estrapolato da *frames* di sistemi di videosorveglianza e inserito in un apposito software di riconoscimento).

Schema n. 1

Come noto, in dottrina non esiste un'unica definizione di "prova digitale"[26]: la letteratura ha fatto riferimento a diverse nozioni nel tempo. Infatti, alcuni autori hanno utilizzato la dizione "*digital*

sconsiglia generalizzazioni aprioristiche». L'ambito di riferimento è quello della cd. "*digital forensics*" (DF), per tale intendendosi «*the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions* (…)». G. Costabile, Digital forensics & digital investigation*: classificazione, tecniche e line guida nazionali e internazionali*, in AA.VV., Cyber forensics *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, (a cura di) S. Aterno, F. Cajani, G. Costabile, D. Curtotti, Giappichelli, Torino, 2021, p. 1, definisce "*digital forensics*" come «un processo teso alla "manipolazione controllata" e più in generale al trattamento dei dati e/o informazioni digitali e/o sistemi informativi per finalità investigative e, più in generale, di giustizia, adottando procedure tecnico-organizzative tese a fornire adeguate garanzie in termini di integrità, "autenticità" e disponibilità delle informazioni e dati in parola. (…) per *digital forensics* s'intende anche il processo investigativo mediante il quale si utilizzano tecniche informatiche atte a raccogliere elementi probatori di varia natura (…), oppure a fornire strumenti utili all'investigatore (nei casi più semplici, ricerca di informazioni sul web come una fotografia dell'indagato oppure l'identificazione di un latitante che usa imprudentemente Facebook, Twitter o altri *social network*)». Cfr. anche G. Peterson, S. Shenoi, *Advances in Digital Forensics*, Springer, Orlando, 2009, B.D. Carrier, *Defining digital forensic examination and analysis tool using abstraction layers*, in *International Journal of Digital Evidence*, 1(2003), 4, pp. 1-12, C. Maioli, *Dar voce alle prove: elementi di informatica forense*, in *Crimine virtuale, minaccia reale*, Franco Angeli, Milano, 2004 e AA.VV., *Questioni di informatica forense*, (a cura di) C. Maioli, Aracne, Roma, 2015. La *computer forensics* invece è la disciplina che si occupa delle tecniche e degli strumenti utilizzati per recuperare gli elementi di prova (digitali) all'interno di un computer. Cfr. S. Aterno, *Digital forensics e scena criminis*, in AA.VV., *Manuale delle investigazioni sulla scena del crimine*, (a cura di) D. Curtotti, L. Saravo, Giappichelli, Torino, 2019, p. 777. Anche nell'alveo della generica categoria della "*digital evidence*" si è soliti distinguere la cd. "*computer-generated evidence*" dalla "*computer-derived evidence*". La prima fa capo alle ipotesi in cui lo strumento informatico sia l'oggetto dell'attività probatoria: in questi casi l'elaboratore viene convenzionalmente utilizzato per la ricostruzione virtuale dei vari accadimenti fattuali attraverso l'analisi e l'elaborazione, con specifici software, dei dati inseriti al suo interno. La seconda, invece, fa capo alle ipotesi in cui il dato digitale estrapolato dall'elaboratore costituisca prova diretta o indiretta di un elemento costitutivo della *res iudicanda*. Cfr. A. Testaguzza, *Digital forensics. Informatica giuridica e processo penale*, Cedam, Milano, 2015, p. 5.

[25] S. Quattrocolo utilizza tale espressione con riferimento ai modelli computazionali utilizzati nel campo della giustizia penale, cfr. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, p. 226.

[26] Sul punto v. D. *La Muscatella, Il trattamento della prova digitale nel sistema processuale penale italiano. Anamnesi e prognosi di una patologia classica, declinata in una (apparente) riforma*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, p. 264. Per un'analisi puntuale delle varie definizioni v. G. Ziccardi, *Scienze forensi e tecnologie informatiche*, in AA.VV., *Investigazione penale e tecnologia informatica*, (a cura di) L. Luparia, G. Ziccardi, Giuffrè, Milano, 2007, pp. 3 e ss. Giova ricordare altresì una suggestiva definizione di L. Cuomo, *La prova digitale*, in AA.VV., *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Luparia, Cedam, Milano, 2017, p. 673, il quale afferma che «le prove digitali, costituite da *record*, file, codici sorgente, tracce digitali, programmi informatici e flussi di *bit*, per la loro natura immateriale variamente rappresentabile, sono raccolte in un luogo virtuale dove perde consistenza la naturale propensione dell'uomo a rapportarsi con il mondo circostante con l'uso dei sensi e, in particolare, con il tatto». Cfr. anche G. Costabile, *Digital forensics & digital investigation: classificazione, tecniche e line guida nazionali e internazionali*, in AA.VV., Cyber forensics *e indagini digitali. Manuale tecnico-giuridico e casi*

evidence" di matrice statunitense, intendendola quale contenitore ove ricomprendere qualsiasi «informazione probatoria la cui rilevanza processuale dipende dal contenuto del dato o dalla particolare allocazione su di una determinata periferica, oppure dal fatto di essere stata trasmessa secondo modalità informatiche o telematiche»[27]. Altri autori l'hanno intesa più generalmente come «qualsiasi fonte di prova memorizzata in strumenti informatici»[28]. L'espressione *digital evidence* è stata così tradotta in "prova digitale", volendo valorizzare l'essenza del dato, frutto di una riproduzione elettronica di numeri. Altra parte della dottrina, invece, ponendo in luce una «strutturale ed intrinseca immaterialità dell'elemento di prova», ha ritenuto più pertinente la locuzione "evidenza di natura digitale"[29]. In letteratura, sono state utilizzate come espressioni sinonimiche di "*digital evidence*" le nozioni di "evidenza informatica" ed "evidenza elettronica"[30]. Da una parte, lo *Scientific Working Group on Digital Evidence* (SWGDE)[31] ha ritenuto che "*digital evidence*" coincida con «qualsiasi informazione, avente valore probatorio, che sia o meno memorizzata o trasmessa in un formato

pratici, (a cura di) S. Aterno, F. Cajani, G. Costabile, D. Curtotti, Giappichelli, Torino, 2021, p. 5, distingue fra "evidenze digitali" ed "evidenze non digitali": le prime sono «quelle fonti di prova memorizzate in strumenti informatici, come le postazioni di lavoro degli utenti, i *server* aziendali, il *Cloud* o altri sistemi cd. informatici/telematici. Questo tipo di evidenze sono caratterizzate da una "carenza di fisicità" che porta ad una maggiore facilità di modifica accidentale durante la fase di acquisizione delle stesse», mentre le seconde sono definite come «quelle fonti di prova che non sono memorizzate in dispositivi informatici come, ad esempio, la stampa di un bollettino falso, del denaro contraffatto, ecc.».

[27] Cfr. L. Marafioti, *Digital evidence e processo penale*, in *Cass. pen*., 2011, p. 4509. La definizione richiama quella di E. Casey, *Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet*, Elsevier, London, 2004, p. 7, secondo il quale "*digital evidence*" corrisponde a «*any data stored or transmitted using a computer that support or refute a theory of how an offence occurred or that address critical elementsof the offense such as intent or alibi*». Una definizione analoga è stata fornita nell'ambito del progetto europeo CyberCrime@IPA in cui è stata stilata una *Electronic Evidence Guide* che identifica la prova informatica come «l'insieme dei dati e delle informazioni che derivano da dispositivi elettronici come i computer e le relative periferiche, le reti di computer, i telefoni cellulari, le fotocamere digitali o altri dispositivi mobili, i dispositivi di archiviazione dati, nonché da internet, [ovvero] informazioni generate, memorizzate o trasmesse mediante dispositivi elettronici che possono essere utilizzate in giudizio». Cfr. E. Colombo, *Una novità dall'Unione Europea per la lotta ai Cybercrimes: una Electronic Evidence Guide*, in *Cass. pen*., 2014, pp. 374 e ss.

[28] Cfr. F. Cajani, *La ricezione della notitia criminis e i primi atti d'indagine*, in AA.VV., *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, (a cura di) S. Aterno, F. Cajani, G. Costabile, D. Curtotti, Giappichelli, Torino, p. 129.

[29] Cfr. F. M. Molinari, *Le attività investigative inerenti la prova di natura digitale*, in *Cass. pen*., 2013, p. 1261.

[30] A sottolineare questo è G. Di Paolo, voce "*Prova informatica*" (diritto processuale penale), in *Enc. Dir*., Annali, VI, Giuffrè, Milano, 2013, p. 736, ove si osserva anche che "*digital evidence*" differisce da "*electronic evidence*" in quanto quest'ultima comprende anche fonti di natura analogica, che ben possono essere digitalizzate ma non nascono in tale formato. Cfr. sul punto S. Mason, *Electronic Evidence: Disclosure, Discovery and Admissibility*, LexisNexis, Londra, 2007, p. 22 in cui la prova digitale è fatta coincidere con tutti quei dati, inclusi quelli derivanti dalle risultanze registrate da apparati analogici e/o digitali, creati, processati, memorizzati o trasmessi da qualsiasi apparecchio, elaboratore elettronico o sistema elettronico, o comunque disseminati a mezzo di una rete di comunicazione, rilevanti ai fini di un processo decisionale. Per un quadro di sintesi delle varie definizioni di "*electronic evidence*" e "*digital evidence*", cfr. G. Vaciago, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli, Torino, 2012, pp. 1 e ss. Giova ricordare che l'espressione "prova informatica" è stata utilizzata dalla giurisprudenza sin dai primi utilizzi del dato digitale nelle aule giudiziarie, cfr. Cass. pen., Sez. I, 19.1.2000, *inedita*. Con riferimento alla locuzione "prova elettronica", essa è stata utilizzata nella Relazione di accompagnamento al d.d.l. n. 2807, in occasione dei lavori preparatori della legge 48 del 2008 (cfr. *infra*).

[31] Costituito nel 1998, il gruppo di lavoro scientifico statunitense sulle prove digitali riunisce le forze dell'ordine, le organizzazioni accademiche e commerciali attivamente impegnate nel campo della medicina legale digitale per sviluppare linee guida e standard interdisciplinari per il recupero, la conservazione e l'esame delle prove digitali. Per maggiori informazioni v. https://www.swgde.org/home (visualizzato in data 14.6.2021).

digitale», dall'altra l'*International Organization on Computer Evidence* (IOCE)[32], seppur abbia accolto una definizione che i più hanno reputato troppo estesa, la considera come «qualsiasi informazione generata, memorizzata e trasmessa attraverso un supporto informatico che può avere valore in tribunale»[33].

Il più recente orientamento giurisprudenziale italiano ha di fatto superato la previgente nozione di documento elettronico, inteso come «qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati ad elaborarli» (art. 491 *bis* c.p.), soppiantata dalla previsione dell'art. 1, lett. *p*), d.lgs. n. 82 del 2005[34], che definisce il documento informatico come «la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti»[35]. In questo senso, sembrerebbe che anche i dati biometrici digitalizzati e generati da dispositivi aventi natura generica o commerciale, seppur non siano il risultato diretto di procedimenti di digitalizzazione regolamentati e non forniscano le doverose garanzie di affidabilità per la loro peculiare genesi, possano essere ragionevolmente ricondotti all'interno della macro categoria dell'evidenza digitale[36].

Peraltro, entro tale *genus*, è possibile distinguere due ulteriori *species*: da un lato la *computer-derived evidence*, in cui l'elaboratore o la rete costituiscono l'oggetto dell'attività probatoria[37], dall'altro l'*electronic evidence* "a genesi procedimentale", concernente le ipotesi in cui l'apparecchiatura informatica risulta essere lo strumento di realizzazione e di conservazione oppure il mezzo dell'operazione probatoria o, ancora, il soggetto dell'operazione dimostrativa. La cifra principale di questa seconda categoria è il fatto che i dati digitali, destinati ad assumere il ruolo

---

[32] Costituito da agenzie governative accreditate statunitensi coinvolte in indagini forensi informatiche, IOCE identifica e discute questioni concernenti la prova informatica, facilita la diffusione internazionale delle informazioni e sviluppa raccomandazioni per i suoi membri. Oltre a formulare standard per il trattamento della prova digitale, IOCE sviluppa servizi di comunicazione tra le agenzie membri e tiene conferenze orientate alla cooperazione fra i diversi membri. V. https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm#:~:text=The%20International%20Organization%20on%20Computer%20Evidence%20(IOCE)%20was%20established%20in,other%20computer%2Drelated%20forensic%20issues. (visualizzato in data 26.6.2021).

[33] Entrambe le definizioni sono riportate in V. Colarocco, T. Grotto, G. Vaciago, *La prova digitale. La casistica civile e penale e gli strumenti di acquisizione in ambito cloud*, Giuffrè, Milano, 2020, p. 41.

[34] CODICE DELL'AMMINISTRAZIONE DIGITALE, reperibile all'indirizzo https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82 (ultimo accesso in data 24.3.2021).

[35] Cfr. D. La Muscatella, *Il trattamento della prova digitale nel sistema processuale penale italiano. Anamnesi e prognosi di una patologia classica, declinata in una (apparente) riforma*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, p. 272 e S. Conti, *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, p. 162. La definizione risulta in linea con quella contenuta nell'art. 1 della Convenzione di Budapest, cui l'art. 2 della l. 48/2008 ha dato piena ed intera esecuzione (cfr. *infra*, nel prosieguo del presente paragrafo), che considera documento informatico «qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione». Cfr. Art. 1, *Convenzione del Consiglio d'Europa sulla criminalità informatica*, reperibile all'indirizzo https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/185.

[36] Cfr. *Towards the European Level Exchange of Facial Images - Legal Analysis for TELEFI project*, reperibile all'indirizzo https://www.telefi-project.eu/sites/default/files/TELEFI_LegalAnalysis.pdf (visualizzato in data 15.12.2021).

[37] In questi termini L. Luparia, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in AA.VV., *Investigazione penale e tecnologia informatica*, (a cura di) L. Luparia, G. Ziccardi, Giuffrè, Milano, 2007, p. 145.

fondamentale di elementi probatori, risultano generati nel corso del procedimento dai cd. "*electronic devices*" in dotazione agli organi inquirenti o ad altri soggetti processuali (e dei loro ausiliari) per l'espletamento delle loro funzioni istituzionali[38].

Evidenza digitale→ "***computer derived evidence"*** nel cui ambito si potrebbero ricondurre le due ipotesi di dato biometrico digitale (b).

↓

L'ipotesi c) misto fra le due categorie.

↓

"***Electronic evidence*****"** procedimentale nel cui ambito si ritiene ragionevole ricondurre l'ipotesi (a).

Schema n. 2

Anche in questo caso[39], la nozione di rappresentazione digitalizzata di un tratto biometrico o di modello elettronico di un dato campione grezzo fatica a conciliarsi con inquadramenti a priori e con le tradizionali distinzioni in tema di prova. Infatti, le specifiche fonti di prova digitale risultano, come già accennato, di difficile collocazione all'interno delle ordinarie categorie probatorie[40]. Peraltro - stante la natura assolutamente versatile della *digital evidence* (o "*digitalized evidence*") - sussiste una sostanziale difficoltà nel conciliare il relativo risultato probatorio con la tradizionale bipartizione tra prove rappresentative e prove indiziarie o critiche[41]. Orbene, la natura multiforme del dato digitale e le caratteristiche intrinseche del tratto biometrico, suggeriscono di evitare generalizzazioni aprioristiche, ma - come già anticipato nel capitolo I, § 1 - piuttosto di abbracciare definizioni più "elastiche"[42]. Su questo terreno, infatti, sembra che una qualsiasi delimitazione epistemologica che voglia entrare nel dettaglio rischi di nascere già "superata". Infatti, si è già fatto cenno alla difficoltà di ricostruire un *iter* univoco di reperimento e di trattamento del dato biometrico, giacché esso muta a seconda dell'informazione che si prende in considerazione. Ne consegue che, anche con riferimento

[38] In questa seconda categoria sono ricomprese le rappresentazioni digitalizzate di dati biometrici e i *templates* generati dagli investigatori o da altri soggetti processuali durante le indagini o il procedimento, in funzione dell'accertamento processuale. Essa pertanto include tanto l'arsenale di strumenti cognitivi a disposizione degli inquirenti in fase investigativa, quanto quelli connessi con l'informatizzazione delle aule di giustizia, e quindi con l'installazione di sistemi elettronici (in parte riconducibili alla categoria della *computer-generated evidence*). G. Di Paolo, voce "*La prova informatica*" in *Enc. Dir*., Giuffrè, Milano, Annali, VI, 2013, p. 740.

[39] Cfr. il capitolo I, § 1.

[40] Infatti, «la natura informatica del dato da cui trarre il risultato probatorio può vertere direttamente sul *thema probandum* sia su un fatto secondario da cui risalire ad un fatto principale (…)». M. Pittiruti, *Digital evidence e procedimento penale*, Giappichelli, Torino, 2017, pp. 8-9.

[41] Cfr. sul punto G. Ranaldi, *Processo penale e prova informatica: profili introduttivi*, in *Diritto Pubblico Europeo online* n. 2/2020, p. 11.

[42] Cfr. M. Daniele, *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen*., 2012, 441 parla di natura giuridica della prova digitale avente contorni ancora non ben definiti.

alla catalogazione normativa del dato biometrico digitalizzato, sussistono vari livelli di complessità a seconda dei diversi oggetti di prova[43]. Infatti, come visto *supra*, esso può trovarsi sottoforma di *template* o rappresentazione digitale ed essere il risultato di un procedimento di digitalizzazione del campione biometrico grezzo, può costituire la derivazione automatica dell'utilizzo di un dispositivo digitale non concepito per un suo impiego all'interno del processo penale; o ancora, esso può essere incorporato semplicemente in un'immagine elettronica ritraente uno specifico dato biometrico. In tal senso, l'unico comun denominatore fra le diverse ipotesi pare attenere alla natura digitale dell'elemento di prova. In effetti, ciò che accomuna le diverse tipologie di dato biometrico digitalizzato e le succitate definizioni di *digital evidence* è proprio la sua fondamentale caratteristica da cui trarre l'informazione probatoria: la sua materialità non immediatamente percepibile[44].

Per vero, la maggioranza delle criticità scaturenti dall'impiego di un elemento di prova incorporato in un supporto e avente natura digitale sussiste proprio nella circostanza che gli elementi ricercati dagli organi investigativi coincidano in «*zeroes and ones of electricity*»[45]. In tal senso, una volta ottenuto l'accesso anche a strumenti di uso quotidiano, quali *computer* e *smartphone*, gli inquirenti hanno a disposizione una quantità enorme di informazioni, inclusi i dati rimossi ai quali nemmeno l'utilizzatore potrebbe, senza una determinata e complessa strumentazione, risalire[46].

A tal proposito, sotto il profilo normativo, riveste un ruolo di fondamentale importanza la Convenzione internazionale di Budapest - come noto - aperta alla sottoscrizione degli Stati membri del Consiglio d'Europa il 23 novembre 2001[47]. Con legge 48 del 2008, l'Italia ha ratificato ed eseguito la Convenzione, introducendo nell'ordinamento il principio cardine della necessità di adottare misure

---

[43] Cfr. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, cit., p. 226.

[44] Come precisato in dottrina, l'immaterialità del dato digitale non deve essere intesa nel senso che le medesime siano prive di fisicità: si tratta infatti di «impulsi elettrici che rispondono ad una sequenza numerica prestabilita e che, convogliati in un supporto informatico dotato di una memoria, originano informazioni intellegibili». Così, M. Daniele, *La prova digitale nel processo penale*, in *Riv. dir. proc*., 2011, p. 284. Per vero, M. Pittiruti, *Digital evidence e procedimento penale*, cit., p. 12, evidenzia che «(…) la peculiare natura dell'incorporamento dell'informazione – a base digitale – non è da sola, tale da far propendere per l'inclusione di uno strumento nel novero delle prove digitali». Per questa ragione, sottolinea l'Autore, è bene distinguere fra prove digitali endoprocedimentali ed extraprocedimentali.

[45] L'espressione è di O. Kerr, *Digital Evidence and the New Criminal Procedure*, in *105 Columbia Law Review*, 2005, p. 291.

[46] Cfr. M. Pittiruti, *Digital evidence e procedimento penale*, cit., p. 144.

[47] La Convenzione sul crimine informatico del Consiglio d'Europa del 2001 contiene una serie di previsioni, dirette ad adeguare le norme ai crimini commessi tramite le nuove tecnologie e incidenti sia sull'assetto sostanziale, sia su quello procedurale (in materia di mezzi di ricerca della prova, giurisdizione e cooperazione giudiziaria). Il riferimento normativo più importante ai fini della presente trattazione è l'art. 19 par. 3 che prescrive di «adottare misure legislative o di altra natura necessarie per consentire alle competenti autorità il sequestro o l'apposizione di vincoli analoghi su dati informatici […] dovranno includere il potere di: a. sequestrare o sottoporre ad analogo vincolo un sistema informatico, una parte di esso o un supporto di memorizzazione di dati informatici; b. operare e conservare una copia di tali dati informatici; c. mantenere l'integrità dei dati informatici rilevanti memorizzati: d. rendere inaccessibili o rimuovere quei dati informatici dal sistema informatico presso il quale erano conservati». CONSIGLIO D'EUROPA, *Convenzione sulla criminalità informatica*, Budapest, 23.11.2001, p. 11.

tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione[48]. Si tratta di operazioni di investigazione informatica comprendenti cinque fasi che consistono nella individuazione, nella acquisizione, nella conservazione, nella analisi e nella presentazione della *digital evidence*[49] (cfr. *infra* il § 1.2). Questo, ovviamente, al fine di tutelare quelle garanzie di riservatezza e di difesa dell'imputato che potrebbero venire compromesse «da un'incondizionata ed indiscriminata acquisizione probatoria non sorretta da parametri normativi predefiniti»[50]. Le difficoltà che il trattamento dei dati biometrici digitalizzati impone al processo penale, infatti, sono tali da rischiare quantomeno di ripensare l'impostazione logico-costruttiva di alcune disposizioni del codice di procedura penale e da richiedere un particolare adattamento per coloro che se ne servono, dovendosi interpretare i costrutti normativi classici alla luce di un'attività per sua stessa natura volatile e farraginosa. Le nuove tecnologie digitali hanno posto in luce l'esigenza della "certezza delle regole", seppur connotate da una certa flessibilità per essere sempre adattabili al progresso scientifico, principalmente per l'individuazione dei dati che poi costituiranno l'oggetto su cui l'organo giudicante sarà chiamato a fondare la propria valutazione, con un contestuale abbandono di eventuali presunzioni di conoscenza assoluta da parte degli esperti del settore, ostative di una corretta analisi del linguaggio fornito dalla *information technology* (cfr. *infra* il capitolo III, § 1.1)[51].

[48] Invero, l'assetto normativo attuale risulta il frutto di un percorso evolutivo iniziato con la l. 23.12.1993, n. 547 e poi sviluppatosi attraverso la legislazione di contrasto alla pedopornografia (l. 15.2.1996, n. 66 e l. 3.8.1998, n. 269), il "pacchetto" antiterrorismo del 2005 (d.l. 27.7.2005, n. 144, convertito con modificazioni dalla l. 31.7.2005, n. 155) e, infine, la legge di ratifica della Convenzione di Budapest del 2001 (l. n. 48/2008). Per un commento in generale sulla legge 48/2008 cfr. F. Resta, *La disciplina acquista maggiore organicità per rispondere alle esigenze applicative*, in *Guida al dir*., 2008, fasc. 16, p. 52, G. Marcoccio, *Convention on Cybercrime: novità per la conservazione dei dati*, in *www.interlex.it*, L. Piccotti, *La ratifica della Convenzione del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir.pen.proc*., 2008, p. 700 e L. Luparia, *I profili processuali*, in *Dir. pen. proc*., 2008, pp. 717 e ss.

[49] Cfr. G. Paolozzi, *Relazione introduttiva*, in AA.VV., *Dimensione tecnologica e prova penale*, (a cura di) L. Luparia, L. Marafioti, G. Paolozzi, Giappichelli, Torino, 2019, p. 3.

[50] Cfr. A. Testaguzza, *Digital Forensics*, cit., p. 9.

[51] Lo studio di questo settore è affidato alla *computer forensics* che si occupa della preservazione, dell'identificazione, dell'acquisizione, della conservazione e della documentazione dei contenuti degli elaboratori elettronici o dei sistemi informativi in generale, allo scopo di evidenziare prove a fini di indagine. L. Cuomo, *La prova digitale*, in AA.VV., *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Luparia, Cedam. Milano, 2017, p. 674. Cfr. anche A. Testaguzza, *Digital forensics. Informatica giuridica e processo penale*, Cedam, Milano, 2015, p. 10. Molto opportunamente si è notato che il tema delle prove informatiche ripropone ed acutizza alcune delle criticità tipiche insite nella *scientific evidence* (cfr. *infra* il capitolo III, § 1.1), tra cui «il rischio di una sopravalutazione giudiziale dei dati raccolti, il pericolo di alterazione e manipolazione del materiale probatorio raccolto e la possibilità di una incontrollata introduzione nel processo di scienza "spazzatura" (*junk science*)». L. Luparia, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in AA.VV., *Investigazione penale e tecnologia informatica*, (a cura di) L. Luparia, G. Ziccardi, Giuffrè, Milano, 2007, p. 137. Sul punto, cfr. anche O. Dominioni, *La prova penale scientifica*, Giuffrè, Milano, 2005.

1.1. Le principali caratteristiche della prova digitale (immaterialità, dispersione, promiscuità, ubiquità, modificabilità)

Una volta posto in luce il rapporto intercorrente fra il cd. "corpo elettronico" e la categoria della *digital evidence*, si ritiene opportuno passare in rassegna le principali caratteristiche di quest'ultima, attribuibili in via esegetica anche al dato biometrico digitalizzato.

In primis, sussiste un carattere di sostanziale immaterialità insito di per sé nell'evidenza digitale[52]. Ciò che conferisce il particolare «pregio tecnico»[53] a questi dati è la rilevante versatilità nel trattamento tecnologico che li rende di semplice memorizzazione e comunicazione. Tuttavia, la loro forte duttilità costituisce anche la loro intrinseca vulnerabilità[54]. Per tale ragione, come si vedrà meglio *infra* (cfr. il § 1.2), nella generalità dei casi l'analisi del dato avviene non sull'originale ma sulla copia forense.

Un altro carattere fondamentale è la rilevante fruibilità processuale che dipende dal costante incremento della diffusione dei sistemi informatici e della digitalizzazione delle conoscenze nella società moderna, con le sempre più frequenti occasioni di interconnessione tra il mondo fisico e quello digitale[55]. Da tali tratti discendono ulteriori caratteristiche che creano non pochi inconvenienti in rapporto alla loro acquisizione processuale. Innanzitutto, si pensi al rischio di dispersione: i dati digitali possono trovarsi potenzialmente dislocati in *server* o *personal computer* molto distanti tra loro. Ne consegue la necessità che il legislatore detti regole precise al fine di individuare la competenza degli organi inquirenti per evitare che si sovrappongano diversi procedimenti in relazione agli stessi episodi criminosi, anche coinvolgendo autorità e organi inquirenti esteri[56]. A tal proposito, la l. 48 del 2008 ha affrontato la questione della dispersione considerando unicamente l'ordinamento italiano: la scelta è stata semplicemente quella di affidare le indagini inerenti i reati di cui all'art. 51 co. 3 *quinquies* c.p.p. alle procure «presso il tribunale del capoluogo del distretto nel cui ambito ha sede il

[52] Cfr. R. Flor, *La Corte di giustizia considera la direttiva europea 2006/24 sulla cd. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. proc*., 2009, 403, evidenzia come l'inarrestabile rivoluzione informatica e la sua «esasperata velocità evolutiva» abbiano «trasformato i dati e le informazioni in "beni immateriali" di inestimabile valore». Cfr. anche L. Cuomo, *La prova digitale*, in AA.VV., *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Luparia, Cedam. Milano, 2017, p. 675, F. Palmiotto, *Le indagini informatiche e la tutela della riservatezza informatica*, in *www.lalegislazionepenale.it*, 1.7.2019, p. 2, F. Siracusano, *La prova informatica*, cit., p. 2, AA.VV., *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations*, cit., p. 14 e S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, pp. 3 e ss. e pp. 121 e ss.

[53] Cfr. A. Testaguzza, *Digital forensics. Informatica giuridica e processo penale*, Cedam, Milano, p. 7.

[54] Cfr. A. Testaguzza, *Digital forensics*, cit., p. 7.

[55] Cfr. C. Sarzana di S. Ippolito, *Informatica, internet e diritto penale*, Giuffrè, Milano, 2010, pp. 7 e ss.

[56] Cfr. M. Daniele, *La prova digitale nel processo penale*, in *Riv. dir. proc*. 2/2011, p. 285.

giudice competente»[57]. La dottrina maggioritaria rimane peraltro alquanto dubbiosa che un tale obiettivo sia stato raggiunto con la normativa in esame[58].

Ulteriore tratto tipico è la promiscuità[59]. Infatti, tale categoria di dati può trovarsi collocata in spazi virtuali enormi e pieni di informazioni di qualsiasi tipo. Non è raro che i dati predetti si trovino insieme a dati del tutto irrilevanti rispetto alla fattispecie di reato e capita molto di frequente che siano attinenti alla vita privata dell'indagato o di altre persone del tutto estranee. In tal senso, le indagini che coinvolgono la ricerca di dati biometrici digitali sono quasi sempre potenzialmente in grado di pregiudicare la riservatezza degli individui; questo perché l'analisi dei sistemi informatici «può rivelare il contenuto di intere esistenze: abitudini, opinioni politiche, preferenze di ogni genere»[60]. Come è già stato suggerito in dottrina, al fine di proteggere la riservatezza dei soggetti, una possibile via da percorrere potrebbe essere quella di una più rigida regolamentazione della facoltà di accesso ai sistemi informatici[61]. Tuttavia, le scelte del legislatore non sono andate in tale direzione: infatti, come si vedrà meglio *infra* (cfr. il § 1.3), le indagini aventi ad oggetto evidenze digitali sono state configurate come ispezioni, perquisizioni e sequestri, disposti anche dal pubblico ministero o, nei casi di urgenza, dalla stessa polizia giudiziaria[62].

Il dato digitale è poi potenzialmente ubiquo, sì da non renderne, talvolta, agevole la corretta e univoca localizzazione[63].

L'immaterialità del dato elettronico determina anche un'altra caratteristica, ossia la sua congenita modificabilità[64]. Un file comune, come un'immagine in formato jpg, comprende circa un milione di bit: la modifica di uno solo di essi può comportare un mutamento irreversibile del file. Infatti, perché il dato sia alterato è sufficiente che venga aperto una sola volta con intuitive conseguenze per la sua rilevanza probatoria. In generale, i dati biometrici digitalizzati contenuti in un sistema informatico, come – più in generale – le prove digitali, risultano potenzialmente alterabili da parte di chiunque ne

---

[57] Cfr. H. Belluta, *Cybercrime e responsabilità degli enti*, in AA.VV., *Sistema penale e criminalità informatica*, (a cura di) L. Luparia, Giuffrè, Milano, 2009, p. 100 e ss., L. Luparia, *I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della Convenzione sul cybercrime*, in AA.VV., *Le nuove norme sulla sicurezza pubblica*, (a cura di) S. Lorusso, Cedam, Padova, 2008, p. 65.

[58] Cfr. M. Daniele, *La prova digitale nel processo penale,* cit., p. 286, sostiene che la norma in esame non sia in grado di creare una titolarità esclusiva della raccolta della prova digitale a favore delle procure distrettuali. Inoltre, non è stato istituito alcun organo centrale analogo alla Direzione nazionale antimafia e antiterrorismo, con la conseguenza che il coordinamento è soggetto al buon volere delle procure di volta in volta coinvolte nelle indagini con lo strumento del collegamento disciplinato dall'art. 371 c.p.p.

[59] Cfr. F. Ruggieri, *Profili processuali nelle investigazioni informatiche,* in AA.VV., *Il diritto penale dell'informatica*, (a cura di) L. Picotti, Cedam, Padova, 2004, p. 158 e F. Siracusano, *La prova informatica*, cit., p. 2.

[60] Cfr. M. Daniele, *La prova digitale nel processo penale,* cit., p. 288.

[61] Cfr. R.E. Kostoris, *La lotta al terrorismo e alla criminalità organizzata tra speciali misure processuali e tutela dei diritti fondamentali nella Risoluzione del XVIII Congresso internazionale di diritto penale*, in *Riv. dir. proc*. 2010, p. 330.

[62] Artt. 352 co. 1 *bis* e 355 c.p.p.

[63] Cfr. F. Siracusano, *La prova informatica*, cit., p. 2.

[64] Cfr. M. Daniele, *La prova digitale nel processo penale, cit.*, p. 292.

venga in contatto[65]: il rischio di dolose contraffazioni e manipolazioni a causa dell'impiego di tecniche non espressamente formalizzate è altissimo. Da ciò discende che, al fine di poter utilizzare informazioni decisive in giudizio, risulti essenziale garantirne l'autenticità. Per tale ragione, si ritiene particolarmente significativo proteggere l'evidenza digitale lungo la cd. *chain of custody*, sino al momento in cui viene resa disponibile al giudice del dibattimento (cfr. *infra* il § seguente)[66]. Infatti, solo l'applicazione di adeguati presidi debitamente tracciati in appositi report consente di dotare l'evidenza digitale del riconoscimento della «resistenza informatica alle contestazioni»[67].

1.2. La *digital evidence* e la sua efficacia probatoria: l'individuazione, l'acquisizione, la conservazione, l'analisi e la presentazione

Chiarito il rapporto intercorrente fra il dato biometrico digitalizzato e la macro categoria della *digital evidence* e passate in rassegna le principali caratteristiche di quest'ultima, si ritiene utile soffermarsi sui principali passaggi previsti per il trattamento del dato digitale a fini giudiziari.

Scopo dell'elaborazione di una *chain of custody* è quello di fornire determinati elementi regolamentati, utilizzabili in un procedimento penale[68]. La prima attività da considerare una volta individuata l'evidenza digitale interessata è l'acquisizione della "copia forense"[69], finalizzata a cristallizzare a fini probatori il contenuto di un dispositivo digitale o di un sistema informatico[70].

---

[65] «Qualunque ingresso in un sistema informatico, anche se effettuato con le metodiche più avanzate, può alterare i dati in esso contenuti, generando mutazioni che, anche se minimali, rischiano di risultare decisive se riguardano circostanze fattuali rilevanti ai fini dell'affermazione della responsabilità dell'imputato». M. Daniele, *La prova digitale nel processo penale*, *cit*., p. 296.

[66] Sul punto cfr. E. Casey, *Digital evidence and computer crime*, Elsevier, London, 2004, pp. 169 e ss., L. Bartoli, *La catena di custodia del materiale informatico: soluzioni a confronto*, in *Anales de la facultad de derecho*, 33, 2016, pp. 146-147. Inoltre, sull'importanza di adottare adeguate modalità di custodia delle tracce, si v. in giurisprudenza Cass. pen., Sez. I, 14.3.2007, n. 15117 in *CED Cass* n. 236391 e, in dottrina, con riferimento all'informatica forense in generale, cfr. G. Faggioli, A. Ghirardini, *Computer Forensics*, Apogeo, Milano, 2009, i quali ritengono la catena di custodia un «presupposto necessario per permettere al giudice sia la verifica nel dettaglio della metodologia utilizzata dall'esperto di *computer forensics* nel compimento delle diverse operazioni, sia la decisione in merito all'utilizzabilità della prova in giudizio e, in caso affermativo, la sua idoneità o meno a provare i fatti ai quali si riferisce». Infine cfr. F. Giunchedi, *Le malpractices nella digital forensics. Quali conseguenze sull'inutilizzabilità del dato informatico?*, in *Arch. Pen*., 2013, 3, p. 826 e G. Caria*, Le quattro fasi dell'analisi forense:identificazione, acquisizione, analisi*, in AA.VV., *Investigazioni digitali*, (a cura di) M. Iaselli, Giuffrè, Milano, 2020, pp. 3 e ss.

[67] Cfr. G. Ziccardi, *L'avvocato hacker. Informatica giuridica e uso consapevole (e responsabile) delle tecnologie*, Giuffrè, Milano, 2012, p. 418.

[68] Cfr. M. Daniele, *La prova digitale nel processo penale*, *cit*., p. 293, R. Brighi, M. Ferrazzano, *Digital forensics: best practices and perspectives*, in AA.VV., *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations*, cit. pp. 15-16 e G. Caria*, Le quattro fasi dell'analisi forense:identificazione, acquisizione, analisi*, in AA.VV., *Investigazioni digitali*, (a cura di) M. Iaselli, Giuffrè, Milano, 2020, p. 6.

[69] La fase di individuazione è piuttosto complessa, in quanto se il reperto non viene individuato prontamente, si espone per un tempo maggiore al pericolo di inquinamento. Ulteriore aspetto da tenere in considerazione durante questa fase è la corretta conservazione ed imballaggio del supporto su cui sono registrati i reperti.

[70] «Le tracce elettroniche consistono in informazioni e dati conservati o trasmessi dalle apparecchiature digitali che, per la loro natura immateriale, possono essere facilmente alterati, danneggiati o distrutti. Il reperto informatico, per i suoi contenuti digitali, è fedelmente riproducibile e il suo esame deve avvenire su una copia onde evitare alterazioni, inquinamenti, contaminazioni o

L'operazione consiste, infatti, nella realizzazione di un'immagine *bit* a *bit* del contenuto del supporto, che consente poi di operare la successiva analisi forense su un *hard disk*[71]. Proprio in relazione alla delicatezza della presente fase, la precedente individuazione dovrebbe essere accuratamente documentata, al fine di garantire l'autenticità lungo l'intero ciclo di custodia. Esso riveste particolare importanza per quei dati biometrici digitalizzati che, non essendo il risultato di un procedimento di digitalizzazione a partire da un campione grezzo, registrano e conservano direttamente un tratto biometrico rilevante ai fini dell'accertamento del reato. Per esempio, ogni volta che s'intenda trattare filmati di videosorveglianza al fine di estrapolare un determinato *frame* per eseguire confronti fisionomici dei volti, sarà sempre necessario eseguire una copia forense[72]. Quest'ultima consiste nella duplicazione del contenuto dell'evidenza rappresentata da una sequenza di lettere (a,b,c,d,e,f) e cifre (da 0 a 9), lunga solitamente 64 caratteri, ottenuta applicando un particolare algoritmo di calcolo alla sequenza di *bit* che formano il file originale (o il testo)[73]. Fondamentale a questo punto è la creazione automatica della cd. impronta *hash*[74], la quale verifica che una immagine sia identica all'originale. L'algoritmo non fa altro che scandire sequenzialmente uno dopo l'altro tutti i *byte* che costituiscono il file e ricavare, passo dopo passo, una serie di "impronte intermedie", ciascuna delle quali dipende dalla precedente, ottenendo, al termine della scansione, l'impronta *hash* definitiva[75]. Ogni fase dell'elaborazione è influenzata da quelle precedenti, determinando lo stato di quelle successive, e per

---

contraffazioni dell'originale». L. Cuomo, *La prova digitale, cit*., p. 695. Sul punto v. anche S. Aterno, *Digital Forensics e scena criminis*, in AA.VV., *Manuale delle investigazioni sulla scena del crimine*, (a cura di) D. Curtotti, L. Saravo , Giappichelli, Torino, 2019, pp. 775-806, L. Cuomo, *La prova digitale*, in AA.VV., *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Luparia, Cedam, Padova, pp. 669-771, L. Luparia, G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Giuffrè, Milano, 2007, p. 64, G. Caria, *Le quattro fasi dell'analisi forense:identificazione, acquisizione, analisi, reporting*, in AA.VV., *Investigazioni digitali*, (a cura di) M. Iaselli, Giuffrè, Milano, 2020, p. 8.

[71] Entro tale fase si è soliti distinguere le tracce digitali in due categorie: le "evidenze informatiche" (file testuali, multimediali o di archivio) la cui sola presenza può dare riscontro all'evento e alla condotta di un illecito, e i "programmi", ossia file che necessitano di un'analisi per divenire evidenti. Nel primo caso la data, l'ora, l'utente che ha creato il file, la sua eventuale cancellazione o modificazione possono essere informazioni utili per la ricostruzione del fatto e una corretta attribuzione della responsabilità in capo all'autore del fatto di reato.

[72] Una parte di dottrina sottolinea l'incerta natura della copia forense del dato, ossia del metodo migliore per assicurare la conformità dell'originale e il risultato della copia. Cfr. D. La Muscatella, *Il trattamento della prova digitale nel sistema processuale penale italiano. Anamnesi e prognosi di una patologia classica, declinata in una (apparente) riforma*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, p. 270.

[73] Rimane del tutto anacronistica ogni questione relativa alla distinguibilità tra originale e copia mutuata dal settore cartaceo: la duplicazione elettronica offre esattamente le stesse garanzie di rappresentazione delle informazioni primarie, poiché il documento di partenza e quello finale sono del tutto identici. Cfr. L. Alberini, *Sul documento informatico e sulla firma digitale (novità legislative)*, in *Giust. civ.*, 1998, p. 267.

[74] «(…) l'*hash* è una funzione non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita (…). È come un'impronta digitale per un file e deriva direttamente dal contenuto dell'oggetto da cui è stata generata». G. Caria, *Le quattro fasi dell'analisi forense: identificazione, acquisizione, analisi*, cit., p. 15. Cfr. anche G. Faggioli, A. Ghirardini, *Computer Forensics*, Apogeo, Milano, 2009, pp. 71-73.

[75] Il calcolo di *hash* viene utilizzato anche per dimostrare che l'originale è identico alla copia poiché l'esecuzione dell'algoritmo su un elemento anche minimamente modificato ne segnala l'avvenuta manipolazione. L. Cuomo, *La prova digitale, cit*., p. 697. Per una definizione generale di "algoritmo" v. *infra* il § 2.

questo motivo è sufficiente modificare anche un solo *bit* di tutto il file per ottenere un'impronta *hash* diversa. Ciò viene fatto per garantire la genuinità del dato prodotto e, in particolare, la perfetta integrità del contenuto copiato e da sottoporre ad analisi. Oltre a ciò, la copia del file soddisfa altresì l'esigenza pratica di evitare che l'acquisizione di tale contenuto agli atti di indagine non riveli dati riservati, relativi all'indagato o a terzi, che nulla hanno a che fare col reato per cui si procede[76].

La legge 48/2008 ha modificato diverse disposizioni del codice di procedura penale in materia di ispezioni (art. 244, co. 2), perquisizioni (art. 247, co. 1-*bis*) e sequestri (art. 254-*bis*), prevedendo, a seconda dei casi, l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione o l'utilizzo di una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità.

In ogni caso, la principale *quaestio* in tema di copia forense di un dato biometrico digitalizzato è rappresentata dalla natura ripetibile o irripetibile di questa fase, giacché solo in quest'ultimo caso possono invocarsi le garanzie difensive previste dall'art. 360 c.p.p. (cfr. *infra* il § 1.4)[77]. Anche se si avrà modo di tornare sul punto, giova anticipare che, mentre la dottrina risulta piuttosto altalenante, considerando tale attività ripetibile[78], irripetibile[79], ovvero diversamente qualificabile a seconda delle circostanze del caso concreto, la giurisprudenza ha generalmente optato per la tesi della normale ripetibilità[80]. Secondo l'orientamento maggioritario della Corte di cassazione, tale operazione «non comporta alcuna attività di carattere valutativo su base tecnico scientifica, né determina alcuna alterazione dello stato delle cose, tale da recare un pregiudizio alla genuinità del contributo conoscitivo in prospettiva dibattimentale. È assicurata, infatti, in ogni caso, la riconducibilità di informazioni identiche a quelle contenute nell'originale»[81], con l'ulteriore elemento di complicazione che, secondo la Corte, non esistendo «ad oggi, uno standard prestabilito per la metodologia di trattamento ed analisi delle prove informatiche, l'eventuale alterazione dei dati informatici – e, quindi, la loro inutilizzabilità – a seguito di operazioni effettuate sugli *hard disk* o su altri supporti informatici, costituisce oggetto di un accertamento di fatto da parte del giudice di merito che, se congruamente motivato, non è

[76] Cfr. G. Carlizzi, *La prova tecnologica nel processo penale*, in AA.VV., *Dimensione tecnologica e prova penale*, (a cura di) L. Luparia, L. Marafioti, G. Paolozzi, Giappichelli, Torino, 2019, p. 82.

[77] Come noto, le garanzie consistono nel diritto di preavviso dell'indagato, della persona offesa e dei rispettivi difensori di assistere al conferimento dell'incarico all'esperto, di partecipare agli accertamenti e di fare osservazioni, con l'ausilio di consulenti eventualmente nominati.

[78] Cfr. L. Cuomo, *La prova digitale*, cit., pp. 701 e ss.

[79] Cfr. L. Luparia, G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Giuffrè, Milano, 2007, pp. 154 e ss.

[80] Per esempio cfr. Cass. pen., Sez. II, 4.6.2015, n. 24998 in *CED Cass* n. 264286.

[81] Cfr. Cass. pen., Sez. II, 16.6.2015, n. 24988 in *CED Cass* n. 264285, conforme a Cass. pen., Sez. I, 9.3.2011, n. 17244, *inedita* e a Cass. pen., Sez. VI, 6.2.2020 in *CED Cass* n. 278808.

suscettibile di censura in sede di legittimità»[82]. Per vero, la fase di acquisizione è la più delicata in assoluto: la copia deve presentare tutti i *bit* del dato digitale[83].

Al momento in Italia non esistono delle *Standard Operating Procedures* (SOP) comuni a tutte le forze di polizia[84]. Generalmente, si fa riferimento a linee guida internazionali dalle quali è dato trarre *check lists* operative[85]. Più nel dettaglio, sono prese in considerazione:

- ISO/IEC 27037:2012 ("*Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*") pubblicate nel 2012[86];

- "*Good practice guide for Computer-Based Electronic Evidence*" (ACPO – *Association of Chief Police Officers*, UK, 2012)[87];

- "*Guidelines for Best Practice in the Forensic Examination of Digital Technology*" prodotta dall'ENFSI – *European Network of Forensic Science Institute*, (2015)[88];

- "*Guidelines on digital forensics*" del NIST –*National Institute of Standards and Technology*, (2014)[89];

- "*Electronic Evidence Guide*" (EEG) del Consiglio d'Europa (2013)[90];

- "*Model Standard Operating Procedures for Computer Forensics*" del *Scientific Working Group on Digital Evidence* (2011)[91].

Lo scopo delle summenzionate linee guida è senza dubbio quello di preservare tutti i dati digitali al fine di non modificare direttamente o indirettamente la fonte di prova. Per tale ragione, chi vi accede deve possedere la competenza tecnica e la conoscenza giuridica necessaria a spiegare in dettaglio i

---

[82] Così Cass. pen., Sez. II, 16.6.2015, n. 24998 in *CED Cass* n. 264285.

[83] Cfr. D. La Muscatella, *Il trattamento della prova digitale nel sistema processuale penale italiano. Anamnesi e prognosi di una patologia classica, declinata in una (apparente) riforma*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, p. 273.

[84] Cfr. S. Aterno, *Digital Forensics e scena criminis*, in AA.VV., *Manuale delle investigazioni sulla scena del crimine*, (a cura di) D. Curtotti, L. Saravo , Giappichelli, Torino, 2019, p. 782, G. Costabile, *Digital forensics & digital investigation: classificazione, tecniche e linee guida nazionali ed internazionali*, in AA.VV., *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, (a cura di) S. Aterno, F. Cajani, G. Costabile, D. Curtotti, Giappichelli, Torino, 2021, pp. 20 e ss. e L. Bartoli, *La catena di custodia del materiale informatico: soluzioni a confronto*, cit., p. 160.

[85] Cfr. G. Ziccardi, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in AA.VV., *Sistema penale e criminalità informatica*, (a cura di) L. Luparia, Giuffrè, Milano, 2009, p. 293 e R. Brighi, M. Ferrazzano, *Digital forensics: best practices and perspective*, cit., pp. 20 e ss.

[86] Reperibili all'indirizzo https://www.iso.org/standard/44381.html#:~:text=ISO%2FIEC%2027037%3A2012%20provides,can%20be%20of%20evidential%20value. (visualizzato in data 19.5.2021).

[87] Reperibile all'indirizzo https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf (visualizzato in data 19.7.2021).

[88] Reperibile all'indirizzo https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf (visualizzato in data 19.5.2021).

[89] Reperibile all'indirizzo https://csrc.nist.gov/News/2014/SP-800-101-Revision-1,-Guidelines-on-Mobile-Device (visualizzato in data 19.7.2021).

[90] Reperibile all'indirizzo https://rm.coe.int/0900001680a22757 (visualizzato in data 19.7.2021).

[91] Reperibili all'indirizzo http://docshare02.docshare.tips/files/27942/279420875.pdf (visualizzato in data 19.5.2021).

passaggi che ha eseguito nell'attività di reperimento del dato biometrico digitalizzato[92]. Tutte le azioni devono essere documentate e registrate in un apposito archivio: ciò consente al giudice e alle parti processuali di valutarle, ma anche di utilizzarle ai fini di ulteriori accertamenti tecnici[93].

La successiva fase di analisi forense è compiuta con metodi che consentono di conservare, documentare, validare e interpretare le informazioni o gli elementi di prova che derivano dai dati digitali, ovvero dalle rappresentazioni di dati biometrici digitalizzati (per esempio filmati di videosorveglianza)[94]. Come già poc'anzi accennato (cfr. *supra*, § 1), in tutti i casi in cui i modelli elettronici e le rappresentazioni digitalizzate di dati biometrici non siano il risultato di procedimenti di digitalizzazione (cfr. il capitolo I, § 2.2), la fase iniziale di analisi di un dato digitale può consistere nel sequestro di un determinato dispositivo, oppure nella copia *in loco* di dati interessanti per l'analisi su un *hard disk* o supporti di proprietà dell'analista forense[95]. Per il suo carattere "ubiquo" il dato biometrico digitalizzato può essere contenuto ovunque. Si tratta di capire quali siano gli strumenti investigativi che consentano la ricerca e l'acquisizione a fini processuali di dati già immagazzinati in *computer*, *smartphone* o *server* aziendali in dotazione della persona sottoposta alle indagini o di terzi. A tal proposito, va sottolineato che la legge 48/2008 (cfr. *supra* il § 1) regolamenta le attività di ricerca e raccolta dei dati digitali riadattando semplicemente gli istituti tradizionali. Come sarà approfondito meglio *infra* (cfr. il § 1.3), con tale normativa sono stati introdotti nel codice alcuni correttivi alle disposizioni in tema di ispezioni, perquisizioni, sequestri, accertamenti urgenti di polizia giudiziaria e acquisizione di plichi di corrispondenza (artt. 244 co. 2, 247 comma 1 *bis*, 254, 256, 269, 352 comma 1 *bis*, 353, 354 c.p.p.) al fine di adeguare le modalità operative alle peculiarità del dato digitale e dell'ambiente informatico[96].

---

[92] Cfr. S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, pp. 146 e 147.

[93] Cfr. S. Aterno, *Digital Forensics e scena criminis*, in AA.VV., *Manuale delle investigazioni sulla scena del crimine*, (a cura di) D. Curtotti, L. Saravo , Giappichelli, Torino, 2019, p. 783.

[94] Le principali attività di analisi sono: a) *text searching*, che consiste nel condurre ricerche di tipo testuale all'interno dei file o delle *directory* e si estende a tutte le strutture del *file system*; b) *image searching*, consiste nella ricerca delle immagini digitali su file di vario formato, inclusi i fotogrammi di file video; c) *data recovery* e *identification* costituita da un primo procedimento di recupero dei dati presenti, cancellati o danneggiati da memorie di massa, da una successiva *data discovery* consistente nel procedimento di scoperta di dati nascosti da una memoria o da file cifrati o protetti in altro modo e, infine, dalla *data carving*, consistente nel tentativo di ricostruire un file danneggiato attraverso il recupero di porzioni di file; d) *metadata recovery* e *identification*, consiste nel recupero di dati comprendenti informazioni di sistema o applicazioni a corredo della struttura del file. Il recupero e l'identificazione dei dati assumono rilevanza in quanto determinano la precisa *timeline* di accesso e di modifica di un file. Cfr. G. Vaciago, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli, Torino, 2012, pp. 98 e ss.

[95] Cfr. L. Luparia, G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Giuffrè, Milano, 2007, p. 63.

[96] Per un approfondimento cfr. *ex multis*, L. Cuomo, *La prova digitale*, in AA.VV., *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Luparia, Cedam, Milano, 2018, pp. 704 e ss.

A questo punto, s'innesta la fase della presentazione del dato digitale. Con riferimento a questa, tra i compiti fondamentali che l'esperto deve assolvere vi è quello di trasformare i dati tecnici individuati in elementi probatori, cioè in informazioni utili e intellegibili per l'accertamento del fatto oggetto di prova. Per esempio, con riferimento all'esame del Dna, una volta riprodotti in via informatica i due elettroferogrammi, l'esperto deve non solo stabilire se essi rappresentino effettivamente i profili genetici contenuti nel campione prelevato all'indagato e nella traccia reperita sulla *scena criminis*, richiamandosi ai principi tecnici seguiti in fase di produzione, ma anche stabilire se tali profili coincidano, ricorrendo ai principi scientifici in materia di corrispondenza genetica[97].

Ciò posto, gli elementi probatori tecnologici non sono i dati tecnici in quanto tali, bensì le informazioni che l'esperto è in grado di fornire circa la loro produzione tecnica e il loro significato scientifico. In tal senso, l'elemento probatorio è qualsiasi informazione ricavabile esaminando un documento o un'immagine, la quale può condurre, attraverso un ragionamento, ad altre informazioni utili per la prova del fatto in giudizio[98].

A questo punto, il giudice deve valutare l'affidabilità epistemologica delle informazioni fornite dall'esperto e ritenerle pertanto attendibili, ossia meritevoli di essere prese per vere ai fini della soluzione della *quaestio facti* (cfr. *infra* il capitolo III, § 1.3). In secondo luogo, l'organo giudicante sarà tenuto a valutare la persuasività delle stesse informazioni, cioè la loro capacità di contribuire, unitamente alle informazioni non specialistiche che emergono in giudizio, alla conferma dell'ipotesi fattuale da provare. Così, volendo riprendere l'esempio dell'esame del Dna[99], il giudice deve valutare, tra l'altro, se il protocollo selezionato dall'esperto per la produzione dell'elettroferogramma corrisponda a quello generalmente applicato nella relativa comunità scientifica e sia stato correttamente seguito; il numero di *matches* tra le diverse coppie di alleli presenti nei marcatori dei due profili genetici corrisponde a quello minimo richiesto nella suddetta comunità al fine di stabilire una corrispondenza tra profili genetici (cfr. il capitolo I, § 3.6); l'individuazione dell'imputato a partire dall'analisi del profilo genetico acquisito sulla *scena criminis* confermi, unitamente ad altri elementi di prova, che egli è effettivamente il responsabile (cfr. il capitolo I, § 2 e il capitolo III, § 1.3.5)[100].

Nonostante siano previsti i suddetti passaggi per il trattamento del dato digitale, risulta tutt'altro che pacifico comprendere quali siano le conseguenze derivanti dalla violazione delle corrette

[97] L'esempio riguarda reperti di Dna digitalizzati, cfr. G. Carlizzi, *La prova tecnologica nel processo penale*, in AA.VV., *Dimensione tecnologica e prova penale*, (a cura di) L. Luparia, L. Marafioti, G. Paolozzi, Giappichelli, Torino, 2019, p. 88.

[98] Cfr. M. Chiavario, *Diritto processuale penale*, Utet giuridica, 2019, p. 427. Sul significato di un *matching* fra dati biometrici digitali rispetto all'oggetto di prova cfr. *infra* il capitolo III, § 1.1.1.

[99] L'esempio è preso da G. Carlizzi, *La prova tecnologica nel processo penale*, cit., p. 89.

[100] Per esempio ricavabili da riprese di videosorveglianza presenti in quel determinato luogo grazie alle quali è possibile compiere una verifica di compatibilità fra i volti.

metodiche scientifiche[101]. Secondo un indirizzo interpretativo giurisprudenziale[102] e una parte di dottrina[103], l'inosservanza delle regole previste nella *chain of custody* non sarebbe riconducibile all'inutilizzabilità, di talché potrebbe rilevare solo nel momento della valutazione della prova. All'opposto, un diverso orientamento sostiene che la violazione delle regole tecniche dovrebbe determinare l'inutilizzabilità delle evidenze elettroniche raccolte[104]. Quest'ultima opzione ermeneutica poggerebbe sulla valorizzazione della portata dogmatica dell'art. 189 c.p.p. nell'ambito del vaglio giudiziale di idoneità dei nuovi strumenti volti ad assicurare un accertamento attendibile e sull'estensione dei limiti, già insiti nel sistema codicistico, di estromissione dal processo di ogni materiale inquinato, in grado di alterare la ricostruzione dei fatti di reato (cfr. il capitolo III, § 1.2)[105]. Tale situazione di incertezza costituisce lo specchio della considerevole difficoltà di applicare le tradizionali categorie concettuali alle descritte, inedite tecniche investigative digitali. Oltre a ciò, occorre riflettere su un ulteriore fattore: le regole previste per la *chain of custody* del dato digitale possono essere considerate efficaci per garantire l'affidabilità del trattamento del tratto biometrico digitalizzato, il quale, come visto, presenta ulteriori profili di complessità derivanti dalle sue caratteristiche ontologiche (cfr. il capitolo I, §§ 1.2 e ss.)? Vien da domandarsi se non sia più efficace costruire un'apposita "*biometric chain of custody*" basata sì sulle analogie con le caratteristiche principali della *digital evidence* (cfr. *supra* i §§ 1 e 1.1), ma tenendo conto delle peculiarità della disciplina alla base e delle differenze fra i diversi tratti biometrici considerati (cfr. il capitolo I, §§ 3 e ss.)[106].

[101] Cfr. G. Di Paolo, voce "*Prova informatica*", in *Enc. dir.*, Giuffrè, Milano, 2016, p. 760 e F. Giunchedi, *Le malpractices nella digital forensics. Quali conseguenze sull'inutilizzabilità del dato informatico?*, in *Arch. pen.*, 2013 (3), pp. 821 e ss.

[102] Sul punto cfr. Trib. Bologna, 22.12.2005, n. 1823, relativa al caso "Vierika", in *Diritto dell'Internet*, 2005, 153, con nota di L. Luparia. Tale sentenza costituisce una delle prime decisioni in materia di *digital forensics* in Italia. Uno dei passaggi più importanti del Tribunale di Bologna è stato il seguente: «non è compito del giudice determinare un protocollo relativo alle procedure informatiche forensi, ma semmai verificare se il metodo utilizzato dalla polizia giudiziaria nel caso in esame abbia concretamente alterato alcuni dei dati ricercati». Con riferimento alla valutazione del dato digitale da parte del giudice e, più specificamente, del dato biometrico digitale cfr. il capitolo III, § 1.3.4.

[103] Cfr. G. Braghò, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in AA.VV., *Sistema penale e criminalità informatica*, (a cura di) L. Lupària, Giuffrè, Milano, 2009, p. 191.

[104] Cfr. L. Luparia, *Computer crimes e procedimento penale*, in AA.VV., *Trattato di procedura penale*, (diretto da), G. Spangher, *Modelli differenziati di accertamento*, (a cura di) G. Garuti, Utet giuridica, Torino, 2011, pp. 374 e ss., C. Conti, *Il volto attuale dell'inutilizzabilità: derive sostanzialistiche e bussola della legalità*, in *Dir. pen. proc.*, 2010, pp. 790 e ss.

[105] Cfr. L. Luparia, *Computer crimes e procedimento penale*, cit., pp. 374 e ss.

[106] In questo senso cfr. N. Bartlow, *Establishing the digital chain of evidence in biometric systems*, West Virginia University, 2009, reperibile su https://www.proquest.com/openview/413bb58439ecb06d19dea4028422886a/1?cbl=18750&loginDisplay=true&pq-origsite (visualizzato in data 2.12.2021).

1.3 La *Digital Forensics* in Italia: aspetti normativi. Le norme del codice di procedura penale introdotte con l. 18.3.2008, n. 48

Dopo aver analizzato i passaggi della *chain of custody* applicabili anche ai dati biometrici digitalizzati nonostante gli imprescindibili limiti dovuti al carattere generale delle varie fasi di protezione del dato, è ora possibile dare definizioni più nitide ai principali istituti processuali "ritoccati" dalla riforma del 2008[107]. Com'è facilmente intuibile, la maggior parte di essi non ha interessato il "corpo elettronico" scaturente da procedimenti regolamentati di digitalizzazione. Infatti, come noto, gli istituti di ispezione, perquisizione e sequestro - *post* intervento normativo della l. 48/2008 - hanno ad oggetto evidenze digitali in quanto tali[108] e non campioni biometrici grezzi trasformati successivamente in rappresentazioni digitali per comparazioni endoprocedimentali. Si ritiene, in ogni caso, che i tre principi fondamentali recepiti dalla normativa nazionale valgano per tutte le tipologie di dati considerati (cfr. *supra* il § 1): tutelare la genuinità del dato originale; impedire l'alterazione della fonte di prova originaria; acquisire il dato tramite procedure che assicurino la conformità della copia prodotta nel corso delle operazioni all'originale informazione digitale[109]. Trattasi di cautele che hanno trovato un solido fondamento nel sapere tecnico-scientifico, costituendo la traduzione giuridica del cd. "blocco in scrittura" durante la riproduzione del dato originale e della validazione della copia forense con la successiva verifica del risultato tramite l'impronta di *hash* (cfr. *supra* il § 1.2).

Venendo alla trattazione degli istituti processuali direttamente interessati dalla novella, il legislatore ha introdotto specifiche garanzie soprattutto nell'ambito dei mezzi di ricerca della prova. Più nel dettaglio, come accennato poc'anzi, la riforma ha interessato l'ispezione e la perquisizione, anche su iniziativa della polizia giudiziaria, l'"inedito" sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni e, infine, gli accertamenti urgenti sulle cose[110].

---

[107] «L'entrata in vigore della legge 18 marzo 2008, n. 48 ha rappresentato un fondamentale passo per l'adeguamento del sistema processual-penalistico italiano agli standard europei in materia di raccolta, conservazione e utilizzo delle prove digitali. Infatti, la legge in questione ha ratificato la Convenzione di Budapest in materia di criminalità informatica ed ha, quindi, introdotto modifiche al codice penale ma soprattutto al codice di rito, prevedendo anche nuove disposizioni. In particolare, l'art. 8 della legge modifica le disposizioni del Libro III Titolo III del Codice di procedura penale (relativo ai mezzi di ricerca della prova), mentre l'art. 9 interviene su quelle del Libro V Titolo IV (relativo alle attività a iniziativa della polizia giudiziaria), adeguando la normativa esistente alla nuova realtà digitale». S. Conti, *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, p. 162.

[108] Cfr. lo schema n. 1: b) "evidenza automaticamente generata" per es. da un dispositivo IoT (per es. uno *smartphone*); c) riproduzione digitale di un dato biometrico trattata da un "dispositivo tecnico specifico" (per es. un volto estrapolato da *frames* di sistemi di videosorveglianza e inserito in un apposito software di riconoscimento).

[109] Cfr. D. La Muscatella, *Il trattamento della prova digitale nel sistema processuale penale italiano. Anamnesi e prognosi di una patologia classica, declinata in una (apparente) riforma*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, p. 270.

[110] Cfr. D. La Muscatella, *Il trattamento della prova digitale nel sistema processuale penale italiano. Anamnesi e prognosi di una patologia classica, declinata in una (apparente) riforma*, cit., p. 270. La dottrina è solita distinguere fra investigazioni informatiche palesi offline e investigazioni informatiche occulte online. Nella prima classe rientrano le ispezioni, le perquisizioni e i sequestri

Nello specifico, l'art. 244 co. 2 c.p.p. – così come modificato dalla l. 48 – impone che «i rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica» possano essere disposti anche in relazione a sistemi informatici o telematici, purché vengano adottate «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»[111]. In tal modo, il testo della disposizione è divenuto più "sintonico" con le indagini compiute su dispositivi digitali[112]. Inoltre, la norma prosegue stabilendo che se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o dispersi o sono stati cancellati, l'autorità giudiziaria può descrivere lo stato attuale, verificando quello preesistente, curando di individuare il modo, il tempo e le cause delle eventuali modificazioni. Si tratta di operazioni aventi un carattere fortemente valutativo più propriamente riservate alla consulenza tecnica e/o alla perizia[113].

Rimane fermo che il ricorso a tale mezzo di ricerca della prova risulta piuttosto limitato, a favore di un prevalente impiego della perquisizione con successivo sequestro del supporto informatico tramite clonazione dei dati, che permette una più agevole analisi del materiale informatico in tempi meno stringenti e in ambienti attrezzati. L'ispezione ha cominciato a trovare più ampi spazi applicativi nei casi di cd. *live digital forensics* (cfr. *infra* il § 1.4.1), ossia le attività di indagine eseguite su sistemi informatici e telefoni accesi, finalizzati a documentare l'esistenza dei dati digitali presenti nella memoria cd. "volatile"[114].

In modo del tutto analogo, il nuovo art. 247, co. 1 *bis* c.p.p. impone l'osservanza della medesima prescrizione in occasione dell'esecuzione di perquisizioni di sistemi informatici o telematici, che siano disposte quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino al loro interno[115]. Come noto, l'intenzione del legislatore è stata quella di preservare i dati digitali, "smarcando" l'istituto della perquisizione dalla materialità

informatici. Le investigazioni occulte, invece, si sostanziano nelle intercettazioni telematiche, nell'utilizzo di *malware* e di altri sistemi intrusivi dei sistemi informatici, nonché tutta una serie di attività che comportano un accesso occulto ad uno specifico sistema informatico o a sistemi hardware e software distribuiti in remoto al fine di memorizzare ed elaborare i dati digitali. V. F. Palmiotto, *Le indagini informatiche*, cit., p. 3.

[111] Si concorda con M. Senor, *Informatica forense*, in AA.VV., *Manuale di informatica giuridica e diritto delle nuove tecnologie*, (a cura di) U. Pagallo, M. Durante, Utet giuridica, Milano, 2019, p. 254, la quale afferma: «(…) nella moderna ITC society in cui la diffusione e l'utilizzo dei mezzi informatici ha raggiunto livelli altissimi, la prova informatica non è più solamente la prova dei reati cd. puri, ma è qualsiasi prova che possa essere ricavata dall'analisi di un sistema informatico. In questi casi, più che di prove dovrebbe parlarsi di indizi in quanto le attività investigative sono finalizzate a cercare non tanto elementi di prova quanto le tracce che l'autore del reato, ma anche la persona offesa o eventuali soggetti terzi, possono aver lasciato nel mondo reale attraverso il mondo virtuale, tracce idonee a validare un alibi, confermare testimonianze o abbozzare la cornice temporale in cui è stato commesso un episodio criminoso».

[112] La norma dopo la novella è stata così definita da M. Senor, *Informatica forense*, cit., p. 255.

[113] Cfr. M. Senor, *Informatica forense, cit*., p. 255.

[114] Cfr. M. Senor, *Informatica forense, cit.,* p. 255.

[115] L'attività di perquisizione informatica o telematica si traduce nella ricerca di informazioni di interesse investigativo e, dunque, tende al sequestro di file attraverso l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. Cfr. A. Cisterna, *Perquisizioni in caso di fondato motivo*, in *Guida dir*., 2008, p. 66.

insita nel corpo del reato e delle "cose" ad esso pertinenti, che mal si conciliano con l'immaterialità tipica delle prove informatiche[116]. Com'è stato già osservato[117], non v'è chi non veda una chiara sovrapposizione tra l'oggetto delle perquisizioni e quello delle ispezioni con riferimento alle tracce elettroniche: la descrizione normativa degli istituti di ispezione, perquisizione e sequestro si presenta come un vero e proprio *work in progress* nella ricerca della prova[118]. Inoltre, va sottolineato il mancato coordinamento tra la novella in tema di perquisizioni e le norme generali che disciplinano il sequestro che non hanno subito alcuna modifica. Più nel dettaglio, l'art. 252 c.p.p. prescrive che le "cose" rinvenute a seguito della perquisizione sono sottoposte a sequestro: ma se sono sequestrate solo le "cose", si è posta la questione di come sia possibile sottoporre ad un vincolo di indisponibilità i dati, le informazioni, i *templates* e le tracce informatiche *tout court* oggetto di perquisizione[119].

Sempre in tema di perquisizioni, un'altra rilevante modifica è intervenuta nell'art. 352 c.p.p., in cui al comma 1 *bis* il legislatore ha stabilito che gli ufficiali di polizia giudiziaria, nella flagranza di reato e nell'ipotesi di esecuzione di un'ordinanza di custodia cautelare o di un ordine di esecuzione, possano procedere alla perquisizione di sistemi informatici, ancorché protetti da misure di sicurezza. Sembra dunque che gli operatori abbiano la possibilità di accedere ad un sistema violandone le misure di sicurezza per monitorare e/o registrare le attività che vengono compiute mediante il sistema stesso.

Un sistema informatico può fungere da contenitore della prova del crimine, da archivio di dati o, più specificamente, di rappresentazioni digitalizzate di dati biometrici, e da strumento di conservazione delle comunicazioni intercorse tra i soggetti coinvolti per il compimento dell'azione delittuosa. Come noto, il sequestro probatorio ha una precisa finalità di accertamento dei fatti e, per la sua adozione, è indispensabile l'astratta configurabilità di un reato e l'esistenza di un collegamento funzionale del sistema informatico con il fatto illecito[120]. Al sequestro del corpo del reato e delle cose pertinenti ad esso, necessarie per l'accertamento dei fatti, provvede l'autorità giudiziaria con decreto motivato (art. 253 c.p.p.), al fine di tutelare l'integrità, la sicurezza e l'affidabilità dei dati, nel rispetto dei diritti e delle libertà fondamentali. Posto, come visto *supra*, che la riforma non è intervenuta sulla disciplina generale in tema di sequestro, una modifica fondamentale da parte della l. 18.3.2008, n. 48

[116] In argomento, la giurisprudenza ha affermato che le norme in tema di perquisizione di sistemi informatici o telematici si limitano a richiedere l'adozione di misure tecniche e di procedure idonee a garantire la conservazione dei dati informatici originali nonché la conformità e immodificabilità delle copie estratte per evitare il rischio di alterazioni, ma non impongono misure e procedure tipizzate. Cfr. *ex multis*, Cass. pen., sez. III, 28.5.2015, n. 37644 in *CED Cass* n. 265180.

[117] Cfr. M. Senor, *Informatica forense,* cit., p. 257.

[118] «(…) si può passare progressivamente da una preliminare attività di osservazione a una attività di ricerca e, poi, eventualmente, a un ulteriore atto di materiale apprensione tramite sequestro». L. Cuomo, *La prova digitale*, in AA.VV., *Prova scientifica e processo penale,* (a cura di) G. Canzio, L. Luparia, Cedam. Milano, 2017, pp. 677-678.

[119] Fatto salvo il caso in cui essi stessi costituiscano il corpo del reato o cose pertinenti ad esso.

[120] Cfr. L. Cuomo, *La prova digitale*, in AA.VV., *Prova scientifica e processo penale,* (a cura di) G. Canzio, L. Luparia, Cedam. Milano, 2017, p. 681.

è stata quella avente ad oggetto il sequestro di corrispondenza (art. 254 *bis* c.p.p.) nell'ambito del quale si è previsto che, in caso di sequestro disposto dall'autorità giudiziaria o di accertamenti urgenti posti in essere su iniziativa della polizia giudiziaria, aventi ad oggetto dati informatici, occorre procedere - come visto *supra* - alla realizzazione, ove possibile, di un duplicato dell'elemento di prova digitale, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità[121]. A tal proposito, è riconosciuto all'autorità giudiziaria, al fine di esaminare un'ampia quantità di dati i cui contenuti sono potenzialmente rilevanti a fini di indagine, il potere di disporre un sequestro dai contenuti molto estesi, comprendente interi archivi di informazioni o sistemi di videosorveglianza, a condizione che si proceda nel rispetto del principio di proporzionalità e adeguatezza[122]. Peraltro, il difensore, per finalità di garanzia, ha diritto di assistere alle operazioni del sequestro e può interloquire sulle modalità esecutive e sulle cautele da adottare per assicurare l'integrità della fonte di prova[123]. Inoltre, nel verbale devono essere descritte tutte le operazioni da effettuare per il deposito e la custodia delle cose sequestrate: questo per impedire che la traccia digitale possa subire alterazioni o modificazioni per l'azione di agenti fisici dannosi (luci, calore, forze meccaniche etc.).

Ne consegue che, in generale, scopo principale della normativa in esame è stato quello di «preservare la *scena criminis* informatica sia nei casi sempre più frequenti di rinvenimento di sistemi informatici/telematici o *smartphone* accesi e collegati alla rete internet, sia nelle diverse ipotesi di rinvenimento di un *personal computer* spento»[124]. Come sottolineato sopra, in dottrina[125], l'intervento del legislatore è stato apprezzabile nella già delineata prospettiva di introdurre idonee misure per proteggere l'intrinseca fragilità del dato informatico, ma non del tutto esaustivo ove si consideri la

[121] Cfr. L. Cuomo, *La prova digitale*, in AA.VV., *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Luparia, Cedam. Milano, 2017, p. 681.

[122] In applicazione dei principi generali di proporzionalità e adeguatezza delle misure cautelari è stato affermato che è illegittimo il sequestro a fini probatori di un intero sistema informatico in difetto di specifiche ragioni che lo giustificano al fine di evitare una indiscriminata apprensione di tutte le informazioni ivi contenute. Cfr. Cass. pen., sez. IV, 24.2.2015, n. 24617, in *CED Cass* n. 264094. Sul punto cfr. L. Cuomo, *La prova digitale*, cit., p. 682 e L. Bartoli, *Parità delle armi e discovery digitale: qualche indicazione da Strasburgo*, in *www.lalegislazionepenale.it*, 13.1.2022.

[123] Cfr. L. Cuomo, *La prova digitale, cit*., p. 686.

[124] Cfr. S. Aterno, *La convenzione di Budapest e la l. n. 48/2008*, in AA.VV., *Cybercrime, Trattati giuridici Omnia*, (a cura di) A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Utet giuridica, Milano, 2019, p. 1356, che specifica come sia «di facile comprensione infatti la differenza che intercorre tra l'ipotesi in cui si rinviene un sistema informatico spento oppure che quest'ultimo si trovi acceso e funzionante o che per le sue qualità e funzioni sia impossibile da sequestrare o da spegnere. È soprattutto in questa ipotesi che può parlarsi più correttamente di perquisizione informatica o di ispezione e di applicazione dell'art. 247 e 244 c.p.p. […] durante un'attività di perquisizione domiciliare, in caso di ritrovamento di un personal computer spento, si deve procedere ad un comunissimo sequestro del sistema […]».

[125] Cfr. sul punto G. Ranaldi, *Processo penale e prova informatica: profili introduttivi*, in *Diritto Pubblico Europeo – Online*, 2/2020, p. 17.

lacuna rispetto alle sanzioni processuali da applicare nel caso di mancato rispetto delle summenzionate procedure modali che hanno lo scopo di garantire la genuinità dei dati digitali (cfr. il § 1.2)[126].

1.3.1. Sulla ripetibilità o irripetibilità delle operazioni: dalla *digital evidence*…

Prima di approfondire il tema della ripetibilità o meno degli accertamenti tecnici informatici posti in essere dagli organi inquirenti, pare doverosa la seguente premessa. Innanzitutto, bisogna specificare che le analisi forensi presentano varia natura e, per tale ragione, può talvolta risultare complesso ricondurre tutte le operazioni di *forensics* ad un'unica categoria giuridica. Al fine di rendere più agevole la comprensione, può risultare utile concentrarsi sull'analisi di un caso frequente e comune, ossia l'estrazione di un dato dall'*hard disk* di un dispositivo digitale oggetto di sequestro. Invero, il contenuto digitale di un determinato dispositivo elettronico non coinvolge necessariamente l'interazione con lo specifico sistema che ha generato concretamente il documento elettronico o ha proceduto all'archiviazione e alla trasmissione dei dati. I dati digitali per loro natura presentano l'attitudine a migrare da un supporto all'altro, senza che il loro contenuto possa subire rilevanti modificazioni in tale processo[127]. Invero, la copia dell'*hard disk* - come visto *supra*[128]- rappresenta un procedimento che, quantomeno secondo un primo indirizzo interpretativo, riesce a garantire la conservazione, la cristallizzazione e il congelamento dei dati necessari ai fini dell'accertamento del fatto. Pertanto, le operazioni che possono essere compiute dagli organi inquirenti a fronte di un dato biometrico digitalizzato, suscettibile di modificazione o alterazione, implicano un'attività tecnica di conservazione dei dati nella loro integrità e, in caso di urgenza, si procede alla realizzazione di una copia forense su un adeguato supporto in modo da rendere quanto compiuto sempre ripetibile: ciò al fine di salvaguardare l'integrità delle informazioni e il diritto di difesa per verificarne la genuinità e la corrispondenza all'originale. A tal proposito, secondo un primo indirizzo interpretativo dottrinale, le acquisizioni e le analisi forensi possono avvenire attraverso accertamenti tecnici ripetibili, con l'ausilio di specifici strumenti informatici che, se usati correttamente, consentono di ripetere l'accertamento ogni volta ne sorga la necessità, senza alcuna modifica dell'elemento di prova[129]. Le operazioni di accertamento aventi ad oggetto un *template* o un'immagine digitale ritraente un dato biometrico - o, ancora più in generale - materiale digitale[130], seguirebbero così la disciplina contenuta

[126] Cfr. A. Colaiocco, *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria*, in *Arch. Pen*., 1/2019 (online), p. 3, F. Giunchedi, Le *malpractices* nella *digital forensics*. *Quali conseguenze sull'inutilizzabilità del dato informatico?*, in *Arch. Pen*., 2013, 3, pp. 821 e ss.
[127] Cfr. F. M. Molinari, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen*. 3/2013, p. 1262.
[128] Cfr. il § 1.2.
[129] Cfr. L. Cuomo, *La prova digitale,* cit., pp. 700 e ss.
[130] Cfr. L. Cuomo, *La prova digitale,* cit., p. 701.

nell'art. 359 c.p.p. Secondo tale *iter* interpretativo, l'estrazione di copia dei file, e più specificamente, di un modello elettronico da un dispositivo digitale non costituirebbe un atto irripetibile[131], dal momento che non comporta alcuna attività di carattere valutativo su base tecnico-scientifica, né determina alcun tipo di alterazione dello stato delle cose o della memoria del sistema informatico tale da poter danneggiare il contributo conoscitivo nella prospettiva dibattimentale, essendo sempre possibile la riproduzione di informazioni perfettamente identiche a quelle contenute nel file originario[132]. Le operazioni urgenti che possono essere compiute dalla polizia giudiziaria nella gestione di un modello elettronico devono tendere alla conservazione del dato nella sua materialità, al fine di rendere l'operazione di duplicazione ripetibile nel futuro e salvaguardare l'integrità del supporto originale. Secondo questo primo orientamento dottrinale[133], quindi, la valutazione da parte degli organi inquirenti deve necessariamente tenere conto delle circostanze del caso concreto, ragionando in termini di urgenza e non di irripetibilità, per cui non può configurarsi alcuna invalidità qualora l'accertamento in questione sia effettuato senza il preavviso del difensore della persona sottoposta alle indagini.

S'intende qui dare conto anche dell'opposto indirizzo ermeneutico di altra parte di dottrina - peraltro maggioritario - sicuro del fatto che, pur prendendo atto che la l. 48 del 2008 abbia collocato le attività di *computer forensic* nell'ampia categoria delle ordinarie indagini di polizia giudiziaria, costituita da rilievi, accertamenti, perquisizioni e sequestri, tali operazioni andrebbero più ragionevolmente ricondotte nella classe degli accertamenti tecnici irripetibili *ex* art. 360 c.p.p., in quanto è «ancora da dimostrare, in realtà, che le indagini informatiche si possano svolgere senza mutare l'oggetto su cui cadono, così come vorrebbe il legislatore»[134]. Ebbene secondo quest'ultimo orientamento dottrinale, proprio la natura digitale del dato configurerebbe «un'urgenza intrinseca che impone, quantomeno, di verificare caso per caso l'eventuale utilità di una cristallizzazione del risultato

---

131 Cfr. L. Cuomo, *La prova digitale,* cit., p. 702.

132 Inoltre S. Aterno, *Digital forensics e scena criminis*, in AA.VV., *Manuale delle investigazioni sulla scena del crimine*, (a cura di) D. Curtotti, Giappichelli, Torino, 2019, p. 794 aggiunge che «l'accertamento tecnico non ripetibile ai sensi dell'art. 360 c.p.p., pur talvolta utilizzato da alcuni organi inquirenti anche in occasione di grandi processi, non consente una buona difesa soprattutto in presenza di numerosi supporti sotto sequestro, degli stretti tempi in cui le operazioni devono essere svolte e soprattutto a causa delle modifiche reali e concrete del supporto sul quale si compie l'accertamento tecnico. Tale ultima circostanza può comportare un pregiudizio irreparabile per qualsiasi delle parti processuali in quanto in caso di errori compiuti nella fase di acquisizione e/o analisi, ad esempio a sfavore dell'imputato, sarà ben difficile anche per un buon consulente tecnico risalire all'originarietà di un dato ormai compromesso».

133 Cfr. A. Chelo, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, Cedam, Padova, 2014, p. 68.

134 Cfr. M. Daniele, *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen*., 2012, p. 443 il quale aggiunge che « qualunque ingresso in un sistema informatico, anche se effettuato con le tecniche più avanzate, altera i dati in esso contenuti, generando cambiamenti che, anche se minimali, rischiano di compromettere l'accertamento dei fatti». Cfr. anche F. Giunchedi, *Gli accertamenti tecnici irripetibili*, Giappichelli, Torino, 2009, pp. 61 e ss., P. Tonini, *Documento informatico e giusto processo*, in *Dir. pen. proc*., 2009, pp. 405 e ss., L. Luparia, *La disciplina processuale e le garanzie difensive, in Luparia-Ziccardi, Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007, pp. 151 e ss.

probatorio attraverso lo strumento dell'accertamento tecnico irripetibile ai sensi dell'art. 360 c.p.p.»[135], essendo «altissimi i rischi che le prove digitali siano contraffatte o manipolate, volontariamente oppure a causa dell'impiego di tecniche sbagliate»[136].

L'orientamento maggioritario della giurisprudenza risulta allineato con il primo indirizzo dottrinale[137]. Infatti, la Corte di cassazione ha più volte avuto modo di affermare che l'attività di estrazione dei dati elettronici contenuti in un supporto digitale o nella memoria di un dispositivo informatico non costituisce un atto irripetibile, dato che non comporta alcuna attività di carattere valutativo su base tecnico-scientifica, né determina alcuna alterazione dello stato delle cose, tale da recare un pregiudizio alla genuinità del contributo conoscitivo in prospettiva dibattimentale. È assicurata, infatti, in ogni caso, la riproducibilità di informazioni identiche a quelle contenute nell'originale[138]. Analogamente, la lettura di un *hard disk* di un dispositivo digitale non darebbe luogo ad un accertamento tecnico irripetibile, posto che si tratta di un'attività di polizia giudiziaria tesa, anche in presenza di una certa urgenza, all'assicurazione delle fonti di prova.

Si può dire che generalmente non vi sia una prevalenza tecnica netta dell'uno o dell'altro tipo di atto[139]. Ciò che sposta il confine tra un accertamento ripetibile e uno irripetibile è l'accurata acquisizione dei dati dal supporto originale e la possibilità di dimostrare concretamente che i dati della

---

[135] Cfr. L. Luparia, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, in AA.VV., *Investigazione penale e tecnologia informatica*, (a cura di) L. Luparia, G. Ziccardi, Giuffrè, Milano, 2007, pp. 152 ss. Nello stesso ordine di idee, v. M. Daniele, *Il diritto al preavviso della difesa nelle indagini informatiche*, cit., p. 443-444, differenziando tra il caso in cui il preavviso al difensore stabilito dall'art. 360 c.p.p. rischierebbe di vanificare le indagini (quando ad esempio i dati digitali d'interesse rimangono nella disponibilità dell'indagato perché reperibili dallo stesso attraverso internet grazie al cosiddetto *cloud computing* oramai sempre più diffuso), e il caso in cui, a seguito del sequestro del computer, i dati non sono più nella disponibilità di chi potrebbe manipolarli, il che consentirebbe di ritenere applicabile la disciplina degli accertamenti tecnici irripetibili. Con riferimento all'analisi del cd. *cloud computing* si è sviluppata una nuova branca della *computer forensics* e, più specificamente, della *network forensics*, ossia la cd. *cloud forensics*, che ha ad oggetto lo studio di tutte quelle informazioni e quei dati non più presenti sui singoli dispositivi ma depositati nel *cyber spazio* e custoditi da vari gestori, per lo più internazionali. Il *cloud computing* è stato definito dal NIST come un modello per abilitare l'accesso alla rete *on-demand* a un *pool* condiviso di risorse configurabili (es.: rete, *storage*, applicazioni e servizi) che possono essere rapidamente fornite e rilasciate con il minimo sforzo di gestione o interazione con il fornitore di servizi. Più nel dettaglio, il *cloud computing* presenta alcune caratteristiche fondamentali tra cui, un ampio accesso alla rete, un *pooling* di risorse, una rapida elasticità e un servizio misurato. Cfr. G. Costabile, *Le indagini digitali*, in AA.VV., *Cyber forensics e indagini digitali*, cit., pp. 63 e 69.

[136] Cfr. M. Daniele, *La prova digitale nel processo penale*, cit., p. 292.

[137] Cfr. *ex multis* Cass. pen., Sez. I, 25.2.2009, n. 11503 in *CED Cass* n. 243495, Cass. pen., Sez. I, 30.4.2009, n. 23035 in *CED Cass* n. 244454, Cass. pen., Sez. IV, 11.12.2020, n. 1621 in *CED Cass* n. 280293, Cass. pen., Sez. II, 14.4.2021, n. 23766 in *CED Cass* n. 281624.

[138] Cfr. Cass. pen., Sez. V, 16.11.2015, n. 11905 in *CED Cass* n. 266477 e Cass. pen., Sez. II, 1.7.2015, n. 29061 in *CED Cass* n. 264572.

[139] «Non vi è dubbio che il legislatore nel disciplinare gli artt. 359 e 360 c.p.p. poteva essere più chiaro e preciso. Nella disciplina codicistica che descrive i due accertamenti vi è una forte confusione terminologica. Mentre l'art. 359 c.p.p. riconosce al pubblico ministero la facoltà di nominare ed avvalersi di consulenti tecnici ove intenda provvedere ad accertamenti, rilievi segnaletici, descrittivi o fonografici e ogni altra operazione tecnica per la quale sono necessarie specifiche competenze, l'art. 360 c.p.p. opera un rinvio all'articolo precedente senza menzionare ad esempio i cosiddetti "rilievi" e dedicando una specifica regolamentazione ai soli "accertamenti tecnici non ripetibili"». S. Aterno, *Digital forensics* e *scena criminis*, in AA.VV., *Manuale delle investigazioni sulla scena del crimine*, (a cura di) D. Curtotti, Giappichelli, Torino, 2019, p. 793. Cfr. anche E. Aprile, *Le indagini tecnico-scientifiche: problematiche giuridiche sulla formazione della prova penale*, in *Cass. pen*. 2003, pp. 4034 e ss.

copia effettuata siano identici a quelli originali nonché che il supporto digitale originale nel frattempo non sia stato modificato[140]. Da una parte, ferma restando sempre la necessità di valutare caso per caso, non v'è ragione per collocare al di fuori delle competenze dell'uomo medio tutte le operazioni connesse all'utilizzo dei dispositivi digitali e delle loro funzionalità. Ciò che si ritiene assolutamente necessario è appurare le specifiche modalità con le quali vengono svolte tutte le attività di trattamento, vuoi della rappresentazione digitalizzata di un dato biometrico, vuoi del suo modello elettronico, nell'ottica di una piena trasparenza e verificabilità ad opera del destinatario. D'altra parte, occorre prendere coscienza che ormai da tempo gli inquirenti s'imbattono quasi quotidianamente in materiale digitale, oggetto di decisivi spunti investigativi e processuali: ne consegue l'introduzione di un necessario bagaglio di conoscenze professionali estese anche al settore tecnico per tutti gli organi investigativi[141]. Infatti, uno standard di conoscenza minimo degli strumenti informatici/digitali risulta ormai un'imprescindibile esigenza da parte di tutti i componenti delle forze dell'ordine e della magistratura inquirente[142], posto comunque che, *ex* art. 348 co. 4 c.p.p., la polizia giudiziaria possa sempre avvalersi di persone idonee al fine di «compiere atti od operazioni che richiedono specifiche competenze tecniche»[143].

1.3.2. …alla *digital proof*

A seconda del diverso inquadramento giuridico, vuoi nell'alveo delle tipiche attività d'investigazione – ispezioni, perquisizioni e sequestri (artt. 352, 354, 244, 247 e 254 *bis* c.p.p.) –[144], vuoi nell'ambito degli accertamenti tecnici, siano essi ripetibili o irripetibili (artt. 359, 360 c.p.p.), il

[140] Cfr. Cass. pen., Sez. V, 16.11.2011, n. 11095 in *CED Cass* n. 266477 e, nello stesso senso, Cass. pen., Sez. V, 3.3.2017, n. 22695 in *CED Cass* n. 270139.

[141] In tal senso cfr. F. M. Molinari, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen*. 3/2013, p. 1264.

[142] Cfr. S. Aterno, *Digital forensics* e *scena criminis*, in AA.VV., *Manuale delle investigazioni sulla scena del crimine*, (a cura di) D. Curtotti, Giappichelli, Torino, 2019, p. 792 afferma che: «salvo in alcune particolari situazioni che possono dipendere anche dalla tipologia di strumenti informatici da acquisire (es.: cellulari, *smartphone*, *ipad*, *tablet*, etc.) l'acquisizione dell'elemento probatorio digitale può avvenire senza dover effettuare un accertamento irripetibile *ex* art. 360 c.p.p. che a volte comporta una *discovery* non gradita all'accusa e dall'altra l'inserimento dei verbali di atti irripetibili nel fascicolo del dibattimento *ex* art. 431, lett. c) c.p.p. con tutte le conseguenze del caso spesso non gradite alla difesa».

[143] A tal proposito, giova ricordare la differenza con l'art. 359 c.p.p. il quale stabilisce che il pubblico ministero, quando procede ad accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze, può nominare e avvalersi di "consulenti". La differenza con le "persone idonee" *ex* art. 348 co. 4 c.p.p. non è solo di denominazione. Mentre queste ultime sono "specialisti tecnici" con funzioni anche meramente esecutive, i "consulenti" si qualificano per le loro competenze scientifiche. A tal proposito, *ex* art. 354 co. 2 c.p.p., il legislatore a seguito della novella n. 48/2008 ha stabilito che, in presenza di un pericolo di modifica o alterazione di dati digitali, la polizia giudiziaria deve adottare le "misure tecniche" per salvaguardarne l'integrità. Per tale ragione sono state elaborate nel corso degli anni una serie di "linee guida" di natura tipicamente "operativa", volte a garantire la genuinità e la non alterazione dei dati informatici nel momento in cui vengono estrapolati dal dispositivo digitale (cfr. il § 1.2).

[144] Cfr. il § 1.3.

trattamento del dato biometrico digitalizzato ha conseguenze intuitivamente differenti nella prospettiva dibattimentale e nella successiva valutazione da parte dell'organo giurisdizionale[145].

Se si ritiene di inquadrare il trattamento dei dati biometrici digitalizzati nella categoria degli accertamenti tecnici *ex* art. 360 c.p.p., i "risultati" - come noto - confluiscono direttamente nel fascicolo nel dibattimento (art. 431 co. 1 lett. *c*) c.p.p.). Con riferimento a tale orientamento interpretativo, è stato affermato che «il riflusso in sede dibattimentale degli esiti di un accertamento tecnico irripetibile» e lo scontro dialettico tra i diversi consulenti tecnici di parte fornirebbe «al giudice gli elementi necessari per scegliere, tra le varie teorie esposte, quella meglio in grado di fornire una risposta soddisfacente agli accadimenti verificatisi»[146]. Detta impostazione solleva alcuni dubbi ermeneutici. Innanzitutto, non si può ignorare quanto è già stato autorevolmente affermato con riferimento alla prova scientifica *tout court* (cfr. il capitolo III, § 1.1), ossia che il ricorso sempre più frequente alla consulenza tecnica e/o perizia finisce molto spesso per introdurre nel giudizio conoscenze fornite da soggetti che non offrono effettive garanzie di indipendenza e sui quali si trasferisce la responsabilità della maggior parte della decisione penale[147]. Inoltre, l'ingresso di un valore di corrispondenza fra due dati biometrici digitalizzati in dibattimento, attraverso i risultati degli accertamenti tecnici irripetibili, andrebbe a erodere quel fondamentale rapporto di immediatezza intercorrente tra il giudice e la prova[148]. Si deve altresì valutare che, essendo indispensabile il preavviso al difensore, l'indagato potrebbe nel frattempo cancellare i *files* compromettenti di cui avesse ancora la disponibilità, vanificando di fatto l'esito delle successive operazioni. Ne consegue che tale meccanismo potrebbe creare diversi rallentamenti nelle indagini per la necessità di concordare con la difesa i tempi e i luoghi di svolgimento degli accertamenti.

Se invece si considera il dato biometrico come mero oggetto di ispezioni, perquisizioni, sequestri e accertamenti tecnici ripetibili allora lo scenario muta parzialmente. In tal caso, gli obiettivi favoriti risultano l'efficacia e la speditezza dell'azione investigativa. Seguendo tale chiave di lettura, si favorisce la separazione delle fasi, riconsegnando al dibattimento la sua tradizionale funzione di sede privilegiata della formazione orale della prova nel contraddittorio tra le parti dinnanzi al giudice.

Rimane ferma l'importanza di una scrupolosa e dettagliata verbalizzazione delle attività poste in essere al fine di realizzare una vera e propria *chain of custody* che cristallizzi e ricostruisca tutto l'*iter* dei reperti sequestrati, con l'indicazione delle date, degli orari, delle operazioni tecniche compiute e

[145] S'intende qui dare conto delle due diverse prospettive, volendo approfondire meglio il tema della valutazione del giudice nel capitolo III.

[146] Cfr. L. Marafioti, *Digital evidence e processo penale*, in *Cass. pen*., 2011, p. 4512.

[147] Per un approfondimento su questo punto, cfr. *infra* il capitolo III. Per il momento, cfr. F. Caprioli, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen*., 2008, pp. 3524-3525.

[148] Cfr. P. Ferrua, *Anamorfosi del processo accusatorio*, in P. Ferrua, *Studi sul processo penale*, vol. II, *Anamorfosi del processo accusatorio*, Giappichelli, Torino, 1992, p. 166.

le sottoscrizioni del personale che se ne è occupato (cfr. *supra* il § 1.2). Quanto al verbale delle operazioni eseguite sulla memoria dell'*hard disk* (*extraction*), essendo dirette al trattamento del cd. file duplicato, e quindi attività ontologicamente ripetibili, esso rimarrà nel fascicolo del pubblico ministero[149]. I dati estratti a seguito di perquisizione informatica, eventualmente sottoposti a sequestro attraverso una copia su adeguato supporto informatico, saranno acquisibili a giudizio come prova documentale nel rispetto di quanto stabilito negli artt. 234 e ss. c.p.p. A questo punto la difesa avrà l'opportunità di chiedere la ripetizione in udienza della perquisizione informatica (o di parti di essa), sia al fine di verificare la correttezza delle operazioni di ricerca eseguite, magari procedendo anche a una nuova analisi, sia per porre in luce nuovi elementi rimasti in ombra nel corso delle attività compiute dagli organi inquirenti in sede di indagine. Ne consegue che la ripetizione in dibattimento della perquisizione renderebbe effettivo quel contraddittorio nella formazione della prova, valore epistemologico del processo[150] e fondamento della decisione giurisdizionale[151]. In questo modo, la *digital evidence* potrà essere considerata ragionevolmente come una *digital proof* ed essere valutata dal giudice in sede di emanazione della sentenza[152].

1.4. Le intercettazioni: quello che le norme (ancora) non dicono

Benché la legge di ratifica della Convenzione di Budapest non sia intervenuta sulla disciplina delle intercettazioni[153], pare opportuno soffermarsi - seppur per brevi cenni - sull'istituto, o meglio su

[149] Sul punto cfr. Cass. pen., SU, 17.10.2006, n. 41281 in *CED Cass* n. 234906 ove si specifica che non va considerato atto irripetibile, e come tale non può essere acquisito al fascicolo per il dibattimento senza il consenso delle parti, il verbale contenente soltanto la descrizione delle attività di indagine, esauritesi con la loro esecuzione e suscettibili di essere descritte in dibattimento, nel contraddittorio delle parti, senza la perdita di alcuna informazione probatoria, per non essere modificabili con il decorso del tempo luoghi, persone o cose rappresentati.

[150] Cfr. A. Nappi, *Libertà e legalità della prova in età moderna e contemporanea*, in *Cass. pen*., 2012, p. 418.

[151] Cfr. F.M. Molinari, *Le attività investigative inerenti la prova di natura digitale*, in *Cass. pen*., 2013, p. 1270.

[152] Cfr. F.M. Molinari, *Le attività investigative inerenti la prova di natura digitale*, cit., p. 1271.

[153] Come noto, «il codice non offre una definizione dell'intercettazione» ma «dal complesso normativo che ne prevede l'autorizzazione e ne regola i presupposti» si è ritenuto possibile ricavare che «l'intercettazione "rituale" consiste nell'apprensione occulta, in tempo reale, del contenuto di una conversazione o di una comunicazione in corso tra due o più persone da parte di altri soggetti, estranei al colloquio». Cass. pen., S.U., 28.5.2003, n. 36747 in *CEDCass* n. 225466. Cfr. anche A. Testaguzza, *Digital forensics. Informatica giuridica e processo penale*, Cedam, Milano, 2015, p.57. Tramite questo mezzo di ricerca della prova le autorità inquirenti possono venire a conoscenza, anche per un lungo periodo di tempo e all'insaputa dei soggetti interessati, di conversazioni e comunicazioni utili – se non spesso indispensabili – per l'accertamento dei fatti. Ancora più intrusivo è il captatore informatico, definito dalle Sezioni Unite della Corte di cassazione nella celebre sentenza Scurato (Cass. pen., S.U., 28.4.2016, n. 26889 in *CEDCass* n. 266905) come un software – del tipo *trojan horse* – installato in un dispositivo digitale (come un computer, un *tablet* o uno *smartphone*), di norma a distanza e in modo occulto, tramite l'invio di una mail, di un sms o un'applicazione di aggiornamento. Per un approfondimento cfr. M. Chiavario, *Diritto processuale penale*, Utet giuridica, Milano, 2019, p. 482, L. Agostino, M. Peraldo, *Le intercettazioni con captatore informatico: ambito di applicazione e garanzie procedurali*, in *Diritto di Internet, digital copyright and data protection*, suppl. fasc. 3/2020, p. 75, D. Curtotti, *Il captatore informatico nella legislazione italiana*, in *Jusonline*, 3, 2017, P. Bronzo, *L'impiego del trojan horse informatico nelle indagini penali*, in *Rivista italiana per le Scienze Giuridiche*, 8, 2017, p. 347, F. Caprioli, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. brasile ira dir. proc. pen.*, 2017, pp. 485 ss.

determinate questioni che, concernendo il concetto di comunicazione in senso lato, sfiorano la disciplina contenuta negli artt. 266 e ss. c.p.p., recentemente riformati[154]. Più nel dettaglio, si intende approfondire due particolari ambiti legati a tale istituto: il riconoscimento informale della voce operato dalla polizia giudiziaria e la modalità *real time* dei software di riconoscimento facciale.

1.4.1 Il riconoscimento informale della voce ad opera della polizia giudiziaria

Nel processo penale, la traccia fonica ha acquisito un indiscutibile valore dovuto all'uso, da alcuni reputato «sfrenato»[155], delle intercettazioni, nel cui ambito si sono annidate alcune problematiche esegetiche. Come già approfondito *supra* (cfr. il capitolo I, § 3.5.1), si ricorre al riconoscimento fonico per attribuire l'identità ai parlanti durante le conversazioni captate[156]. Per tale ragione, risulta fondamentale registrare le specifiche modalità acquisitive del patrimonio ricognitivo finalizzate a garantire la genuinità del risultato probatorio e a minimizzare il pericolo dei cd. "falsi ricordi"[157]. Proprio durante l'ascolto delle intercettazioni telefoniche è possibile che si verifichi un'ipotesi

[154] Per un approfondimento sulla riforma che ha interessato la materia delle intercettazioni cfr. *ex multis* AA.VV., *Le nuove intercettazioni*, (a cura di) M. Gialuz, in *Diritto di Internet, digital copyright and data protection*, suppl. fasc. 3/2020, D. Pretti, *Prime riflessioni a margine della nuova disciplina delle intercettazioni*, in *www.dirittopenalecontemporaneo*, 2018, (1), pp. 189 e ss., C. Conti, *La riservatezza delle intercettazioni nella "delega Orlando"*, in *www.dirittopenalecontemporaneo*, 2017 (3), pp. 78 e ss. Per ulteriori approfondimenti si veda AA.VV., *Nuove norme in materia di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, (a cura di) G. Giostra, R. Orlandi, Giappichelli, Torino, 2018, AA.VV., *Le nuove intercettazioni*, (a cura di) O. Mazza, Giappichelli, Torino, 2018, D. Pretti, *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni*, in *www.sistemapenale.it*, 2020, pp. 71 e ss., G. Pestelli, *La controriforma delle intercettazioni di cui al d.l. 30 Dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità*, in *www.sistemapenale.it*, 2020, pp. 109 e ss.

[155] Cfr. T. Alesci, *Il corpo umano fonte di prova*, Cedam, Milano, 2017, p. 99.

[156] Giova ricordare che la comunità scientifica e gli organi investigativi ripongono molte speranze nella cd. impronta fonica, la quale potrebbe essere in grado di identificare univocamente un determinato soggetto. In data 13.7.2017, si è tenuta una conferenza organizzata dall'Arma dei Carabinieri, intitolata "*La biometria vocale nelle investigazioni*" (cfr. T. Alesci, *Il corpo umano come fonte di prova, cit*., pp. 99-100). In tale occasione il generale Tullio Del Sette ha affermato che: «la realizzazione della banca dati rappresenta una nuova sfida e un passaggio importantissimo. Non pensiamo solo alle intercettazioni ma anche alle conversazioni che si possono trovare sul web e che possono rivelarsi significative ai fini dell'individuazione e del riconoscimento degli autori di diversi reati. Non soltanto reati predatori, di corruzione che avvengono in Italia nell'ambito di una città, mi riferisco anche alla criminalità organizzata transnazionale e al terrorismo internazionale. È già avvenuto che dei terroristi assassini magari con il volto coperto siano stati riconosciuti attraverso il confronto della loro voce con una già riconosciuta e questo attesta che siamo già a un livello molto alto in questo settore. Un settore in cui l'Italia si posiziona tra i paesi più avanzati. Questo avviene un po' per tradizione e un po' per necessità perché noi in Italia, così come la Polizia di Stato e la Guardia di Finanza ci confrontiamo da tanti anni con la criminalità organizzata. Abbiamo cominciato con la necessità di riconoscere le voci nei sequestri di persona degli anni '70 e '80 e nelle attività di contrasto dell'eversione interna e del terrorismo. Questo ci ha spinto tutti a cercare di procedere rapidamente verso nuovi sistemi, nell'individuazione di nuove apparecchiature, nell'utilizzazione degli strumenti più avanzati che ad esempio in America o in altri Stati erano stati messi a disposizione delle forze di polizia più attente. Ci ha spinto anche a inventare qualcosa. Alcuni brevetti, infatti, sono stati registrati da appartenenti al raggruppamento investigazioni scientifiche dei carabinieri».

[157] Cfr. T. Alesci, *Il corpo umano fonte di prova*, cit., p. 99.

borderline di "riconoscimento informale" compiuto dal personale tecnico addetto[158]. Generalmente, l'attribuzione della paternità delle comunicazioni viene effettuata dalla polizia giudiziaria, in virtù di una serie di controlli che tengono conto dell'intestazione dell'utenza o della titolarità della scheda telefonica utilizzata, dell'esame dei tabulati telefonici, dei servizi di appostamento e osservazione dei soggetti presenti in un determinato luogo, ove si sta eseguendo un'intercettazione ambientale. Entro tale scenario, l'identificazione della voce può assumere un ruolo significativo. In tal senso, la giurisprudenza ritiene che la dichiarazione dell'ufficiale che affermi di aver riconosciuto, ascoltando le registrazioni di conversazioni telefoniche, la voce dell'imputato, a lui familiare perché nota per ragioni investigative o per altre circostanze, costituisca un valido indizio[159]. Trattasi di una fattispecie caratterizzata da ricognitori peculiari (la polizia giudiziaria) e un contesto particolare (quello investigativo). Più nel dettaglio, si tratta di un'operazione squisitamente accidentale che avviene durante le attività di intercettazione nel cui ambito non si ritiene possa essere così opportuno disporre un'individuazione. Infatti, l'intercettazione è un mezzo di ricerca della prova tipicamente nascosto: procedere con il riconoscimento della voce captata ai sensi dell'art. 361 c.p.p. potrebbe danneggiare l'attività investigativa in corso.

In altre parole, sembra che, pur trattandosi di un'ipotesi piuttosto rara, sia legittima ed utilizzabile la testimonianza con la quale l'ufficiale di polizia riferisca di aver ascoltato le chiamate captate e di aver identificato l'indagato mediante il suo timbro vocale. Resta ferma la possibilità di verificare l'affidabilità di tali dichiarazioni mediante la *cross examination* e, in caso, chiedendo altresì l'assunzione di una perizia (o consulenza tecnica) fonica.

1.4.2. La modalità *real time* dei software di riconoscimento facciale

Un altro tema peculiare che lambisce la disciplina delle intercettazioni e delle video-registrazioni nel contesto digitale-biometrico è rappresentato dalla modalità *real time* del software di riconoscimento facciale[160]. Tale tecnologia permette l'analisi automatizzata dal vivo e limitatamente ad un'area geografica ristretta di individui, non già rappresentati in immagini statiche, ma ripresi in più flussi video, derivanti da telecamere fisse oppure da dispositivi video portatili come telefoni

[158] Cfr. M. Biral, *L'identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, in *Rivista Italiana di Diritto e Procedura Penale*, fasc.4, 2015, p. 1842 e K. La Regina, *Riconoscimento della voce - brevi note sul riconoscimento della voce nel processo penale*, in *Giur. It.*, 2018, 1, p. 212.

[159] Cfr. Cass. pen., Sez. I, 8.5.2013, n. 35011 in *CED Cass* n. 257209, Cass. pen., Sez. I, 20.9.2007, n. 38484 in *CED Cass* n. 238042, Cass. pen., Sez. I, 6.3.2007, n. 22722 in *CED Cass* n. 236763, Cass. pen., Sez. II, 23.11.2004, n. 47673 in *CED Cass* n. 229909, Cass. pen., Sez. V, 27.10.2004 n. 11921 in *CED Cass* n. 231872. In dottrina cfr. M. Biral, *L'identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, in *Riv. It. di Dir. e Proc. Pen.*, fasc.4, 2015, p. 1842 e T. Alesci, *Il corpo umano fonte di prova*, cit., p. 99.

[160] Si tornerà nuovamente meglio *infra* al § 2.1.1. e al capitolo IV, § 1.3.

cellulari o *body cameras*[161]. I volti presenti nei fotogrammi dei diversi *streams* video vengono comparati mediante un algoritmo di riconoscimento che attinge gli elementi della comparazione direttamente da una banca dati la cui grandezza solitamente è dell'ordine delle centinaia di migliaia di soggetti[162]. Il software "passa in rassegna" ad altissima velocità le immagini custodite in archivio e quelle ignote di provenienza eterogenea (sia catturate dallo *streaming* del video ma anche riprese da telefoni cellulari) alla ricerca di un *match*[163]. Al termine dell'operazione, l'algoritmo restituisce una lista di profili ordinati secondo un punteggio di probabilità basato sul grado di similarità rispetto all'immagine del soggetto da individuare[164]. La corrispondenza del volto ignoto con quello schedato è resa nota all'operatore da un segnale di *alert* generato dall'algoritmo. Sebbene non sia ancora sistematicamente impiegato tra le forze di polizia, trattasi di una forma di captazione particolarmente intrusiva eseguita per scopi di prevenzione, indagine e repressione del reato[165]: una sorta di ripresa *live* di quanti si trovino nelle aree interessate da sovrapporre alle identità di soggetti memorizzati nella *watch list*.

Invero, il legislatore non ha ancora provveduto a disciplinare puntualmente svariati mezzi tecnologici di ricerca della prova ritenuti oggi assolutamente essenziali, seppur oggetto di numerosi dibattiti, tra i quali proprio le videoriprese, con o senza riconoscimento facciale automatico[166].

Si ritiene che il tema possa ragionevolmente accostarsi a quello delle videoregistrazioni, oggetto di una nota sentenza a sezioni unite della Corte di cassazione[167]. Come noto, la Corte di legittimità ha

---

[161] Per un approfondimento sulla modalità *real time* del software di riconoscimento facciale italiano S.A.R.I. nello spettro delle garanzie fondamentali dell'individuo v. *infra* il capitolo IV, § 2.2.3. A questo punto della ricerca si intende anticipare alcune peculiarità di una delle modalità applicative dei software di riconoscimento facciale al fine di proporre un suo inquadramento giuridico.

[162] Cfr. R. Lopez, *La rappresentazione facciale tramite software*, in AA.VV., *Le indagini atipiche*, (a cura di) A Scalfati, Giappichelli, Torino, 2019, p. 243. Per una definizione di "algoritmo" v. *infra* il § 2.

[163] cfr. il capitolo I, § 2.3.

[164] Relazione del Dott. L. Rinella, Direttore di Polizia Scientifica durante il convegno "*Dalle impronte digitali al riconoscimento dell'iride: il corpo umano come oggetto e mezzo di investigazione*", organizzato dall'Università del Piemonte Orientale "A. Avogadro" e la Questura di Alessandria, tenutosi ad Alessandria presso il Dipartimento di Giurisprudenza e Scienze politiche, economiche e sociali, in data 20 novembre 2019.

[165] Come si approfondirà meglio *infra*, l'utilizzo del sistema *Real Time* del software di riconoscimento facciale S.A.R.I. in Italia, ha ricevuto recentemente un parere negativo dall'Autorità Garante per la protezione dei dati personali, perché giudicato non conforme alla normativa sulla privacy. V. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento facciale: Sari Real Time non è conforme alla normativa sulla privacy*, 16.4.2021, in https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575842 (visualizzato in data 16.4.2021).

[166] Cfr. M. Gialuz, *Premessa*, in *"Le nuove intercettazioni legge 28 febbraio 2020, n. 7"*, *Diritto di Internet, digital copyright and data protection*, suppl. fasc. 3/2020, p. 6.

[167] Cass. pen., S.U., 28.3.2006, n. 26795 in *CED Cass* n. 234270. Sul punto v. C. Conti, *Le video-riprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi "riservati"*, in *Dir. pen. proc*., 2006, 11, 1347 e ss., C. Conti, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Diritto penale e processo*, 9/2018, p. 1211, S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, pp. 303 e ss., F. Nicolicchia, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Wolter Kluwer, Milano, 2020, pp. 29 e ss., G. Di Paolo, *"Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione*, Cedam, Padova, 2008, pp. 186 e ss. e A.

stabilito che le videoregistrazioni eseguite in luoghi pubblici, effettuate al di fuori dell'ambito del procedimento penale, vadano incluse nella categoria dei documenti di cui all'art. 234 c.p.p.[168], mentre le medesime, se eseguite dalla polizia giudiziaria a procedimento penale già iniziato, vadano annoverate entro la categoria delle prove atipiche disciplinate dall'art. 189 c.p.p., se rispettose del duplice requisito dell'idoneità ad assicurare l'accertamento del fatto ovvero l'assenza di pregiudizio per la libertà morale della persona[169]. Peraltro, trattandosi di documentazione avente ad oggetto attività investigativa non ripetibile, possono essere allegate al relativo verbale e inserite così nel fascicolo per il dibattimento.

Per contro, le operazioni eseguite all'interno del domicilio o in luoghi assimilabili ad esso[170] sono regolate diversamente a seconda che l'oggetto ritragga comportamenti "comunicativi" o "non comunicativi". A tal proposito, alcune pronunce hanno operato tale distinzione con riferimento alle videoriprese "*live*" da parte della polizia giudiziaria a scopo di indagine, distinguendo fra comportamenti comunicativi (quindi vere e proprie intercettazioni ambientali)[171] e comportamenti non comunicativi (anch'esse vincolate alla preventiva autorizzazione dell'autorità giudiziaria se eseguite in luoghi diversi dal domicilio, ma comunque "riservati")[172]. Infine, l'atto risulta svincolato dal rispetto di particolari formalità esecutive ove abbia ad oggetto condotte non comunicative che hanno luogo in spazi pubblici ovvero aperti o esposti al pubblico. Va osservato che questa distinzione si rivela talvolta artificiosa, perché fondata sulla scissione di uno strumento investigativo in realtà unitario quanto a tipologia, natura, grado e modalità di compressione del bene tutelato. Si è così sottolineato che, spesso, il confine tra meri comportamenti (azioni come ad esempio il confezionamento della droga) e comunicazioni (anche non verbali, come nel caso di gesti o smorfie) possa rivelarsi oltremodo labile, sicché l'utilizzabilità della prova verrebbe ad essere ancorata a parametri evanescenti e impercettibili[173]; senza contare che tale distinzione non si confronta con l'impossibilità pratica di differenziare *ex ante* i diversi tipi di comportamenti.

Camon, *Le Sezioni Unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi*, in *Riv. it. dir. proc. pen*., 2006, p. 1550.

[168] Cfr. Cass. pen., S.U., n. 26795 del 28.3.2006, cit., § 4.

[169] Per una ricostruzione analitica cfr. G. Di Paolo, *"Tecnologie del controllo" e prova penale,* cit., p. 188 e L. Cuomo, *La prova digitale*, in AA.VV., *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Luparia, Cedam, Milano, 2018, p. 738.

[170] Cfr. G. Di Paolo, *"Tecnologie del controllo" e prova penale*, cit., pp. 227 e ss.

[171] Cfr. *ex multis*, Cass. pen., sez. V, 17.11.2015, n. 11419, *inedita*.

[172] Altrimenti, se eseguite in ambito domiciliare inammissibili (e inutilizzabili). Cfr. G. Di Paolo, *"Tecnologie del controllo" e prova penale*, cit., p. 225, L. Cuomo, *La prova digitale*, in AA.VV., *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Luparia, Cedam, Milano, 2018, p. 739 e A. Cabiale, *I limiti alla prova nella procedura penale europea*, Wolters Kluwer, Milano, 2020, pp. 40 e ss.

[173] Cfr. A. Camon, *Le Sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi*, in *Riv. it. dir. proc. pen*., 2006, p. 1550 e O. Mazza, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Diritto Penale Contemporaneo*, 3/2013, pp. 10 e ss.

A questo punto, anche se in Italia l'impiego di tale modalità di riconoscimento da parte delle autorità di pubblica sicurezza risulta attualmente controverso (cfr. *infra* il capitolo IV, §§ 2.1.1. e ss.), un passaggio fondamentale per l'attribuzione univoca dell'identità del soggetto ripreso con modalità *real time*, analogamente a quanto accade con l'applicazione del riconoscimento facciale in modalità applicativa differita (cfr. il capitolo IV, § 1.3), sarebbe costituito dall'analisi morfologica compiuta dall'operatore sul volto che s'intende riconoscere. Tale procedimento avrebbe quantomeno lo scopo di verificare l'attendibilità del riconoscimento automatico compiuto dal software. Tuttavia, si ritiene che tale articolata disciplina interpretativa debba essere ridiscussa alla luce dell'attuale disponibilità di potenti e sofisticati strumenti di controllo. Come è stato osservato, «le tecnologie oggigiorno in uso sono infatti astrattamente idonee a consentire la sorveglianza di tutti gli spostamenti e le attività di un determinato "bersaglio" entro un contesto spazio-temporale potenzialmente illimitato»[174].

Per vero, seppure tali strumenti dotati di tecnologie in grado di attribuire simultaneamente al loro utilizzo l'identità di determinati soggetti non siano ancora oggetto di sistematica applicazione da parte delle forze dell'ordine, la situazione non appare più sostenibile: in un ordinamento fondato sul principio di legalità processuale (art. 111, co. 1 Cost.) non è concepibile delegare alla giurisprudenza e alla dottrina - generalmente con la copertura della soluzione «*passe-partout*» dell'art. 189 c.p.p.[175] - il delicato compito di bilanciare le esigenze di prevenzione e repressione dei reati con la tutela dei diritti fondamentali pregiudicati dalle prove "scientifiche nuove"[176]. Il punto che verrà posto in luce con il successivo capitolo sarà proprio quello di mettere a fuoco le garanzie fondamentali che devono sempre essere riconosciute all'indagato e ai soggetti terzi dinnanzi a questi nuovi strumenti tecnologici (cfr. meglio *infra* il capitolo III, §§ 2 e ss.). Insomma, volendo riprendere l'ammonimento di Stefano Rodotà, secondo il quale «senza una forte tutela del "corpo elettronico", dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo»[177], oggi più che ieri urge dare nuovo vigore al dibattito dedicato alla prova tecnologica e ai diritti fondamentali nel processo penale.

---

[174] Cfr. F. Nicolicchia, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Wolter Kluwer, Milano, 2020, pp. 32 e ss.

[175] Cfr. M. Gialuz, *Premessa*, in *"Le nuove intercettazioni legge 28 febbraio 2020, n. 7"*, *Diritto di Internet. Digital Copyright e Data Protection*, suppl. 3/2020, p. 6.

[176] Cfr. O. Dominioni, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2005.

[177] Cfr. S. Rodotà, *Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, all'indirizzo https://www.privacy.it/archivio/rodo20040916.html (visualizzato in data 6.4.2021).

1.5 Cenni sulla cooperazione giudiziaria internazionale per la raccolta e acquisizione dei modelli elettronici

Un particolare aspetto connesso al tema dell'evidenza digitale di cui si intende dar conto, seppur per brevi cenni, ha ad oggetto la cooperazione giudiziaria europea e internazionale in materia penale[178]. Sussiste una stretta connessione fra l'evidenza digitale e il tema dell'approvvigionamento probatorio transnazionale. Infatti, «in un mondo ormai globalizzato, alla "globalizzazione della criminalità" occorre far fronte con una "globalizzazione della legalità": la cooperazione processuale penale tra gli Stati non può essere limitata a quella tra le loro polizie né finalizzata alla (sola) protezione degli interessi interni, perché questi sono ormai connessi alla protezione degli interessi collettivi di più Paesi»[179].

Sempre più spesso, le attività di ricerca e raccolta di rappresentazioni digitali di dati o loro modelli elettronici travalicano i confini nazionali in quanto i sistemi informatici, o i *providers*, sono situati all'estero[180]. Data la natura transnazionale delle reti di comunicazione, la disciplina processual-penalistica italiana sulle prove digitali deve necessariamente essere esaminata alla luce di un confronto, seppur per brevi cenni, con la normativa sovranazionale ed europea. È evidente che tali questioni possono essere meglio affrontate con l'adozione di adeguate e uniformi misure, sia a livello internazionale che a livello europeo. Fondamentali dunque, entro tale scenario, diventano le attività di cooperazione europea e internazionale anche tra autorità giudiziarie e, in particolare, tra pubblici ministeri e forze di polizia di diversi Stati[181]. Le "nuove" frontiere tecnologiche impongono, quindi,

---

[178] Cfr. F. Siracusano, *La prova informatica*, cit., p. 2, F. Galli, *Information Sharing as a Tool in the Fight against Impunity in the European Union*, in AA.VV., *The Fight Against Impunity in EU Law*, (a cura di) L. Marin e S. Montaldo, Hart Publishing, New York, 2020, pp. 172 e ss., S. Conti, *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, p. 154 e S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 8. Con riferimento specifico al trattamento di dati biometrici finalizzato alla gestione dell'immigrazione e contrasto al crimine e al terrorismo si tornerà meglio *infra* al capitolo IV, §§ 1.5 e ss.

[179] Cfr. G. Ubertis, *Considerazioni generali su investigazioni e prove transnazionali*, in *Cass. pen.*, 2017, 1, p. 50. Sul punto, v. anche S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, pp. 152 e ss.

[180] Si pensi, tra gli altri, ai dati che immettiamo nei *social network*. A. Colaiocco, *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria*, in *Arch. Pen.*, fasc. 1, 2019, S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 159 e M. Daniele, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Rev. Bras. de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, 2019, p. 1279.

[181] Entro tale scenario è possibile riconoscere una "collaborazione orizzontale" tra autorità giudiziarie e di polizia e una "collaborazione verticale" che si esplica in diversi soggetti istituzionali, tra cui Eurojust, organismo europeo di coordinamento giudiziario (cfr. *infra* il § 1.5.1.1.). Anche la polizia giudiziaria dei singoli Stati trova un punto di riferimento, finalizzato ad uno scambio di informazioni più rapido ed incisivo, negli organismi di coordinamento investigativo quali Europol, Interpol e OLAF. Per un approfondimento, cfr. F. Cajani, *La cooperazione internazionale nelle indagini digitali*, in AA.VV., *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, (a cura di) S. Aterno, F. Cajani, G. Costabile, D. Curtotti, Giappichelli, Torino, 2021, pp. 242 e ss.

sfide inedite sotto il profilo della ricerca e della raccolta della prova *ultra fines*. Il Consiglio d'Europa e l'Unione europea rappresentano, in questo ambito, due entità che hanno influenzato e stanno influenzando, con la loro attività e con i loro provvedimenti, la legislazione nazionale in materia di crimini informatici e di raccolta, conservazione e scambio delle prove digitali connesse ad un determinato reato. La loro azione mira a creare un sostrato comune a livello europeo e internazionale e rappresenta una sfida per la realizzazione di un'armonizzazione legislativa tra i vari Paesi europei e gli Stati terzi[182]. Per vero, uno degli obiettivi principali che le più recenti fonti internazionali e di matrice europea hanno cercato di tenere sempre in costante considerazione è la regolamentazione di nuove forme di assistenza e cooperazione aventi ad oggetto gli sviluppi inediti della tecnologia digitale nell'ambito delle indagini penali[183].

1.5.1 (segue) i diversi strumenti normativi

In tal senso, la già menzionata Convenzione di Budapest (cfr. *supra* il § 1) ha dedicato la sua terza parte alle misure di assistenza giudiziaria volte alla ricerca e all'apprensione di evidenze elettroniche immagazzinate in sistemi informatici circolanti nella rete[184]. La *ratio* di fondo è duplice: da un lato spinge verso forme di armonizzazione dei diversi sistemi processuali coinvolti, dall'altro individua alcune regole basiche nell'ambito della cooperazione internazionale. La prima prospettiva muove dalla premessa che le indagini digitali siano soggette alle condizioni e alle tutele previste dal diritto interno di ciascuno Stato, così da fornire un'adeguata protezione ai diritti e alle libertà fondamentali. L'art. 15 par. 2 delimita i confini di questa scelta: il legislatore nazionale deve prevedere una

[182] Cfr. S. Conti, *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, p. 154.

[183] A tal proposito, giova ricordare la recente ratifica da parte dell'Italia del Protocollo di modifica alla Convenzione 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, a Strasburgo il 10 ottobre 2018. In tal senso, la Convenzione svolge un ruolo fondamentale per la diffusione del modello europeo di protezione dei dati a livello mondiale. Più nel dettaglio, «nel Protocollo di modifica viene definito in maniera più specifica il principio di liceità del trattamento (con particolare riferimento ai requisiti relativi al consenso) e viene ulteriormente rafforzata la protezione delle categorie speciali di dati (che vengono al contempo estese a quelle riconosciute come categorie particolari di dati personali nel diritto dell'Unione). La convenzione aggiornata prevede, inoltre, ulteriori garanzie per le persone fisiche alle quali si riferiscono i dati personali trattati (in particolare, l'obbligo di valutare il probabile impatto di un'operazione di trattamento dei dati che si intende effettuare, l'obbligo di adottare le opportune misure tecniche e organizzative e l'obbligo di segnalare gravi violazioni dei dati) e consente di rafforzare i loro diritti (in particolare, trasparenza e accesso ai dati). Sono stati introdotti, poi, nuovi diritti degli interessati: non essere sottoposti a una decisione basata unicamente su un trattamento automatizzato che arrechi un pregiudizio significativo alle persone; opporsi al trattamento e disporre di un ricorso in caso di violazione dei diritti della persona». Per un approfondimento v. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9585156.

[184] Più nel dettaglio, oltre alle cosiddette misure provvisorie (artt. 29 e 30) vi sono altresì la richiesta di assistenza finalizzata alla perquisizione, sequestro o divulgazione di dati immagazzinati in un sistema informatico situato nel territorio dello Stato richiesto (art. 31), l'accesso diretto a dati contenuti in un sistema informatico situato nel territorio di un altro Stato (art. 32), la richiesta di assistenza per la raccolta e la registrazione, in tempo reale, di comunicazioni trasmesse attraverso l'uso di un sistema informatico (art. 34) e la richiesta di assistenza per la raccolta in tempo reale di dati di traffico (art. 33). G. Di Paolo, *Prova informatica*, in *Enc. Dir*., Annali, VI, Giuffrè, Milano, 2013, p. 761.

"supervisione" giudiziaria, limitare l'ambito di operatività delle indagini informatiche, specificare la durata delle stesse, disciplinarne le modalità di svolgimento. Il principio di legalità e la riserva giurisdizionale devono costituire il *fil rouge* di questa particolare ricerca probatoria (art. 15 par. 3).

Con riferimento alle specifiche disposizioni dedicate alla cooperazione transnazionale viene sancito un obbligo di cooperazione (art. 23), inteso come una vera e propria linea guida per l'applicazione e l'interpretazione di tutte le disposizioni convenzionali (cfr. *infra* il § 1.5.2). Si evidenzia un certo *favor* nei confronti di uno scambio spontaneo di informazioni, qualora si ritenga che esse possano essere utili per l'avvio o lo svolgimento di indagini o procedimenti relativi ai reati oggetto della Convenzione (art. 26). All'uopo, ogni Stato deve predisporre un "punto di riferimento" sempre disponibile tra le autorità giudiziarie al fine di garantire un'adeguata assistenza e assicurare l'immediata esecuzione dell'atto rogato (art. 35). Qualora non sussista alcun trattato o accordo di mutua assistenza, l'art. 27 prescrive che ciascuno Stato designi un'autorità centrale responsabile della ricezione delle richieste di assistenza e di risposta alle stesse. Le richieste devono essere eseguite in conformità alle norme indicate dall'autorità giudiziaria richiedente (*lex fori*) sempre che siano compatibili con la legislazione dello Stato richiesto. L'oggetto della domanda può concernere l'adozione di misure provvisorie (artt. 29 e 30) oppure lo svolgimento di vere e proprie attività di indagine (artt. 31-34). Ai sensi dell'art. 29, poi, il cd. *data freezing* costituisce una misura che può essere mantenuta per un periodo non superiore ai sessanta giorni e prodromica all'eventuale successiva richiesta di perquisizione e sequestro. L'invio di una richiesta di congelamento del dato digitale può comportare che lo Stato richiesto scopra che sia coinvolto un *service provider* di un altro Stato. In questo caso, lo Stato richiesto dovrà condividere i dati di traffico con lo Stato richiedente in modo da geolocalizzare il *service provider* e inoltrare una nuova richiesta di assistenza giudiziaria.

L'art. 32 poi, consente la possibilità di accesso diretto ai dati immagazzinati in sistemi informatici situati all'estero senza che sia necessaria alcuna autorizzazione da parte dello Stato ove questi dati sono raccolti, previo consenso della persona «legalmente autorizzata a divulgare i dati». Tale istituto ha ad oggetto i dati pubblicamente disponibili (le cd. fonti *open source*) e le informazioni per cui è del tutto irrilevante il luogo geografico in cui si trovano. Trattasi di un istituto inedito nella pletora dei tradizionali strumenti di cooperazione giudiziaria, che svincola quest'ultima dalle "maglie" della territorialità della prova da raccogliere e dal principio di sovranità. Questi ultimi sono sostituiti piuttosto dall'elemento consensuale direttamente dipendente dalla manifestazione di volontà del "titolare" dello stesso a renderlo accessibile. La *ratio* risulta evidente: dal momento che l'attivazione dei tradizionali strumenti di coordinamento investigativo richiede un *iter* piuttosto lungo e complesso, si consente allo Stato di procedere "da sé". Meno chiaro è il meccanismo di individuazione del titolare

del consenso[185]. Entro tale contesto, infatti, si evidenzia un superamento del principio di mutua assistenza, posta la potenziale ubiquità come uno dei tratti caratterizzanti il dato digitale (cfr. il § 1.2), potendo divenire reperibili in reti informatiche accessibili in qualsiasi luogo[186]. Nonostante la presenza di tale previsione normativa, concordemente con parte della dottrina[187], si ritiene comunque doveroso il ricorso ai tradizionali strumenti di cooperazione internazionale e, in particolare alla rogatoria[188].

Nel più limitato ambito geografico e giuridico dell'Unione europea, il quadro degli strumenti di cooperazione investigativa o probatoria adottabili appare scarno sul fronte delle indagini digitali. Infatti, con riferimento a queste ultime si registra in Europa un'asincrona timidezza nella regolamentazione, inconciliabile con la complessiva preoccupazione del legislatore comunitario riservata all'introduzione di una disciplina dei sistemi di intelligenza artificiale rafforzata, peraltro, ancora di recente (cfr. *infra* il § 2).

1.5.1.1 La direttiva 2016/680/UE

Al fine di garantire lo scambio di dati personali da parte delle autorità competenti all'interno dell'Unione europea per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica, occorre fare riferimento in primo luogo ai principi sanciti nella direttiva 2016/680/UE[189]. In tal senso, le disposizioni che occorre considerare sono contenute negli articoli che vanno dal 35 al 40, per quel che concerne il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, ovvero, nell'art. 50 quanto al dovere di cooperazione fra gli stessi Stati membri. Quest'ultima disposizione non sembra destare particolari problematiche dal punto di vista interpretativo, dal momento che essa stabilisce che ciascuno Stato membro presti assistenza reciproca, adottando tutte le misure opportune al fine di adempiere ad una richiesta di un'altra autorità di controllo senza ingiustificato ritardo, entro un mese dal ricevimento della richiesta.

La normativa concernente lo scambio dei dati personali verso Paesi terzi risulta invece più frammentata. L'articolo 35 prescrive che qualsiasi trasferimento di dati personali oggetto di un trattamento o destinati ad essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, può essere eseguito solo qualora il paese terzo o l'organizzazione

[185] Cfr. M. Pittiruti, *Digital evidence e procedimento penale*, Giappichelli, Torino, 2017, p. 29.
[186] Cfr. F. Siracusano, *La prova informatica*, cit., pp. 7 e ss.
[187] Cfr. M. Pittiruti, *Digital evidence*, cit., p. 29.
[188] Cfr. F. Siracusano, *La prova informatica*, cit. p. 2 pone in luce il fatto che il dato digitale «può non sempre prestarsi a essere adeguatamente gestita attingendo ai tradizionali protocolli dell'assistenza giudiziaria, saldati al principio di territorialità della prova e poco adatti a consentire un accesso rapido ai dati così da assicurare l'inalterabilità».
[189] Cfr. il capitolo I, § 1.2.

internazionale garantisca un «livello di protezione adeguato» (art. 36)[190]. Quest'ultimo parametro è valutato sulla base della sussistenza o meno di diversi requisiti, tra i quali giova ricordare l'esistenza di uno stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale avente la competenza nel garantire e vigilare sul rispetto delle norme in materia di protezione dei dati[191]. Ai sensi dell'art. 40 della direttiva, si prescrive che la Commissione e gli Stati membri si dotino di meccanismi di cooperazione internazionale al fine di agevolare l'applicazione efficace della legislazione sulla protezione dei dati personali, prestare assistenza reciproca e promuovere la cooperazione a livello internazionale per l'applicazione della legislazione sulla protezione dei dati personali.

Il quadro normativo risulta, invero, più complicato e più frammentato di come descritto. A tal proposito, l'articolo 2 paragrafo 3 lettera *b*) stabilisce che le disposizioni contenute nella direttiva non si applichino ai trattamenti di dati personali "effettuati da istituzioni, organi, uffici e agenzie dell'Unione"[192]. A titolo esemplificativo, è l'ulteriore regolamento (UE) 2018/1727[193] avente ad

[190] Cfr. S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 93.

[191] Il Comitato europeo per la protezione dei dati (*European Data Protection Board*) ha pubblicato le Raccomandazioni 01/2021 aventi ad oggetto ulteriori specificazioni circa il concetto di adeguatezza. Esse sono reperibili all'indirizzo https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_it (visualizzato in data 23.9.2021).

[192] Il trattamento dei dati da parte di Europol è disciplinato dal regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI, reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0794. Ai fini della presente ricerca, si ritiene utile richiamare alcune disposizioni contenute nel regolamento. Tra queste, il considerando n. 25, il quale prescrive che Europol dovrebbe assicurare che a tutti i trattamenti di dati personali a fini di analisi operativa (ossia *ex* art. 2 «tutti i metodi e tecniche con cui sono raccolte, conservate, trattate e valutate informazioni allo scopo di sostenere le indagini penali») sia assegnata una finalità specifica. Peraltro, il considerando specifica altresì che «affinché possa svolgere la propria missione, Europol dovrebbe essere autorizzata a trattare tutti i dati personali ricevuti per individuare collegamenti tra svariati settori della criminalità e indagini e non soltanto all'interno di un unico settore della criminalità». Vi è poi, il considerando n. 33, il quale specifica che «tutti gli Stati membri sono affiliati all'Interpol. Per svolgere la propria missione, l'Interpol riceve, archivia e diffonde dati nell'intento di aiutare le competenti autorità di contrasto a prevenire e combattere la criminalità internazionale». E ancora, la stessa disposizione evidenzia l'importanza di un costante promovimento di «un efficace scambio di dati personali, assicurando nel contempo il rispetto dei diritti e delle libertà fondamentali attinenti al trattamento automatizzato dei dati personali». In particolare, questi ultimi sono generalmente definiti dall'art. 2 come «qualsiasi informazione riguardante un interessato». Infine, l'art. 18 del regolamento prescrive che, al fine di perseguire gli obiettivi indicati nell'art. 3 («Europol sostiene e potenzia l'azione delle autorità competenti degli Stati membri e la loro reciproca cooperazione nella prevenzione e nella lotta contro la criminalità grave che interessa due o più Stati membri, il terrorismo e le forme di criminalità che ledono un interesse comune oggetto di una politica dell'Unione (…)»), Europol può trattare informazioni inclusi dati personali. Il par. 2 specifica poi che «i dati personali possono essere trattati solo a fini di: a) controlli incrociati diretti a identificare collegamenti o altri nessi pertinenti tra informazioni concernenti: i) persone sospettate di aver commesso un reato di competenza di Europol o di avervi partecipato, o che sono state condannate per un siffatto reato; ii) persone riguardo alle quali vi siano indicazioni concrete o ragionevoli motivi per ritenere che possano commettere reati di competenza di Europol; b) analisi strategiche o tematiche; c) analisi operative; d) facilitazione dello scambio d'informazioni tra Stati membri, Europol, altri organismi dell'Unione, paesi terzi e organizzazioni internazionali».

[193] Cfr. il regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio, del 14 novembre 2018, che istituisce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust) e che sostituisce e abroga la decisione 2002/187/GAI del Consiglio PE/37/2018/REV/1, reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32018R1727.

oggetto la disciplina di Eurojust, che contiene le disposizioni sulla specifica libera circolazione dei dati personali trattati da Eurojust. Vi sono, poi, le regole in materia di trattamento dei dati personali contenute nella decisione 2007/533/GAI (artt. 56-65)[194] e nel Trattato di Prüm (artt. 24-32) che permettono alle parti lo scambio di dati relativi ai profili del Dna e delle impronte digitali, firmato nel 2005, al di fuori del quadro istituzionale dell'Unione europea e incorporato nel diritto dell'Unione europea con le decisioni 2008/615/GAI[195] e 2008/616/GAI[196], dedicato alle "*Disposizioni generali relative alla protezione dei dati*".

Pertanto, sussisterebbero forti dubbi su quale sia l'esatta normativa da applicare nelle situazioni in cui, per esempio, il dato potrebbe essere custodito in molteplici supporti (digitali e analogici)[197]. Com'è stato osservato in dottrina, il quadro giuridico risulta «complesso da ricostruire e incerto, specialmente quando viene in rilievo il trattamento di dati che potrebbero essere soggetti a più di una di queste normative in materia di *data protection*»[198]. Il permanere di norme specifiche sulla protezione dei dati negli strumenti che disciplinano i sistemi Europol, Eurojust o Prüm implica un considerevole sforzo per gli interpreti al fine di comprendere quali disposizioni debbano essere applicate al caso concreto.

1.5.1.2. Il Trattato di Prüm e le decisioni 2008/615/GAI e 2008/616/GAI

Riguardo specificamente ai profili del Dna e ai dati dattiloscopici, il quadro normativo di riferimento per l'attuazione della cooperazione internazionale giudiziaria e di polizia appare forse il meno complesso nella sua individuazione ma non nella sua applicazione concreta. Si è già fatto brevemente cenno *supra* al Trattato di Prüm[199], stipulato il 27 maggio 2005 tra Belgio, Germania,

---

Giova anche in questo caso richiamare le disposizioni che si ritengono utili ai fini della presente ricerca. In primo luogo, Eurojust è autorizzato a trattare alcuni dati personali relativi a persone che, in base alla legislazione nazionale degli Stati membri interessati, sono sospettate di aver commesso o di aver partecipato a un reato di competenza di Eurojust o che sono stati condannati per tale reato. L'elenco di tali dati personali dovrebbe includere numeri di telefono, indirizzi di posta elettronica, dati di immatricolazione dei veicoli, profili di Dna (parte non codificante), fotografie e impronte digitali. Giova specificare che nel regolamento non è previsto che Eurojust possa effettuare un confronto automatizzato dei profili Dna o delle impronte digitali (considerando n. 34, Allegato II).

[194] Decisione 2007/533/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II), reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX%3A32007D0533. Si tornerà su questo *infra* al capitolo IV, § 1.5.1.

[195] Decisione 2008/615/GAI del Consiglio, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera, del 23 giugno 2008, in GU L210, 6 agosto 2008, pp. 1–11.

[196] Decisione 2008/616/GAI del Consiglio del 23 giugno 2008 relativa all'attuazione della decisione n. 2008/615/GAI sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera.

[197] Campione grezzo, rappresentazione digitale ovvero *template*.

[198] Cfr. G. Rugani, *La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della direttiva (UE) 2016/680: frammentazione ed incertezze applicative*, in *Freedom, Security & Justice: European Legal Studies Rivista quadrimestrale on line sullo Spazio europeo di libertà, sicurezza e giustizia* 2019, n. 1, p. 87.

[199] Cfr. il capitolo I, § 3.6.2.

Spagna, Francia, Lussemburgo, Paesi Bassi e Austria[200]. L'accordo, come visto, nasce con lo scopo di rafforzare la cooperazione tra gli Stati nella lotta al terrorismo, alla criminalità transfrontaliera e all'emigrazione illegale, tramite alcune specifiche aree di intervento: a) la raccolta e lo scambio di informazioni relative ai profili del Dna; b) la raccolta e lo scambio di informazioni sulle impronte digitali; c) lo scambio dei dati relativi ai registri di immatricolazione dei veicoli; d) le misure finalizzate a prevenire reati terroristici ed infine e) le misure dirette a contrastare l'immigrazione illegale. A pochi anni di distanza dalla sua stipula, nell'ambito delle istituzioni europee, sono state poi approvate le due succitate decisioni 2008/615/GAI e 2008/616/GAI che hanno pienamente integrato nel quadro normativo europeo le disposizioni contenute nel Trattato di Prüm[201]. La prima, finalizzata a migliorare lo scambio di informazioni, in un'ottica di cooperazione, prevede che gli Stati membri si concedano reciprocamente diritti di accesso ai rispettivi schedari automatizzati di analisi del Dna, ai sistemi automatizzati di identificazione dattiloscopica e ai dati di immatricolazione dei veicoli. In particolare, il meccanismo di cooperazione si basa su un sistema "*hit/no hit*" che consente allo Stato membro che effettua la consultazione in uno schedario automatizzato, di chiedere in un secondo tempo allo Stato membro che gestisce lo schedario i dati personali specifici corrispondenti e, se necessario, ulteriori informazioni mediante procedure di assistenza reciproca[202]. Più nel dettaglio, per i dati concernenti i profili del Dna e le impronte digitali, il sistema Prüm ha predisposto un meccanismo di accesso online ai soli dati di indice. Questi ultimi contengono solamente la parte di Dna non codificante o i dati dattiloscopici con un generico riferimento, ma non consentono in alcun modo l'identificazione di un individuo. In questo modo, nel caso in cui, a seguito di una consultazione automatizzata dei dati, fosse riscontrabile una concordanza, gli Stati interessati sarebbero posti nelle condizioni di richiedere ad un altro Stato il dato completo, al fine di compiere le analisi necessarie. La trasmissione dei dati personali e delle informazioni ulteriori avviene in base «al diritto nazionale della Parte contraente richiesta, comprese le disposizioni relative alla collaborazione giudiziaria» (artt. 5 e 10 della decisione n. 615).

[200] Per un approfondimento cfr. M. Bargis, *Note in tema di prova scientifica nel processo penale*, in *Rivista di diritto processuale*, 2011, pp. 54 e ss., G. Di Paolo, *La circolazione dei dati personali nello spazio giudiziario europeo dopo Prüm*, in *Cass. pen.*, 2010, pp. 1969 e ss. e M. Gialuz, *La tutela della privacy nell'ambito del trattamento domestico dei dati genetici e della cooperazione informativa*, in AA.VV., *Banca dati e accertamento penale*, (a cura di) L. Marafioti, L. Luparia, Giuffrè, Milano, 2010, pp. 177 e ss.

[201] Cfr. *supra* il § 1.5.1.1. Le decisioni sono attualmente oggetto di una proposta di modifica che si approfondirà meglio *infra* al capitolo IV, § 4.3, cfr. Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council, COM/2021/784 final, reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A784%3AFIN&qid=1639141496518 .

[202] Cfr. il considerando n. 10 della decisione 2008/615/GAI del Consiglio, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera.

La seconda decisione, invece, concerne il potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera[203]. Anche questa materia, riguardando la lotta alla criminalità e le garanzie di sicurezza, è rimasta appannaggio esclusivo degli Stati membri e si è basata sull'introduzione di un insieme di specifiche tecniche comuni, oggetto degli Allegati alle decisioni. Oltre al "principio di disponibilità" fondamentale durante tutto il procedimento di *information sharing*[204], altrettanto importante è divenuto il rispetto e la garanzia del diritto alla protezione dei dati personali in seguito all'introduzione del regolamento (UE) 2016/679 e della direttiva 2016/680/UE[205]. Tuttavia, l'ampia discrezionalità lasciata ai singoli Stati membri e la rilevante diversità fra le normative nazionali, hanno indotto, da una parte, a introdurre un livello minimo di garanzia oggetto di necessaria tutela da parte di tutti i legislatori nazionali, assicurato anche da un controllo esercitato specificamente dal Consiglio dell'UE[206], e dall'altra, a lasciare intatto il potere in capo agli Stati membri di stabilire proprie disposizioni nazionali in materia di raccolta, conservazione, cancellazione e scambio di dati[207]. Le differenze sostanziali in termini di operatività delle banche dati nazionali e il cd. *degree of connectivity with other Member State's databases* hanno spinto le istituzioni dell'UE a riflettere sull'esigenza di modificare il meccanismo esistente perché giudicato ancora del tutto inefficiente[208].

1.5.1.3. Cenni sulla direttiva 2014/41/UE

A distanza di quasi dieci anni dalla legge italiana di ratifica della Convenzione di Budapest, il d.lgs. 21.6.2017, n. 108, in attuazione della direttiva 2014/41/UE, ha introdotto la disciplina dell'ordine europeo di indagine penale (da qui in avanti OEI), il cui scopo principale è stato quello di sostituire lo strumento della rogatoria nello spazio euro-unitario, «rimuovendo alcuni dei tradizionali ostacoli che possono frustrare l'esigenza delle autorità giudiziarie e inquirenti di acquisire prove in altri Stati membri»[209]. Ancora dopo, con il d.lgs. 3.10.2017, n. 149 è stato riformato il libro XI del codice di

[203] Infine, con decisione del Consiglio 2010/482/UE del 26.7.2010 è stato concluso un accordo fra UE ed Islanda e Norvegia, al fine di applicare alcune disposizioni delle decisioni 2008/615/GAI e 2008/616/GAI.

[204] Per un approfondimento cfr. M. Gialuz, *La tutela della privacy nell'ambito del trattamento domestico dei dati genetici e della cooperazione informativa*, cit., pp. 178 e ss.

[205] Cfr. *supra* il § precedente.

[206] L'art. 25 della decisione 2008/616/GAI stabilisce che il Consiglio ha il compito di effettuare un controllo preventivo, subordinando la possibilità dello Stato membro di scambiare i dati e avere accesso alle banche dati di altri Stati membri.

[207] Per un approfondimento cfr. L. Scaffardi, *Next Generation Prüm e le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, in *federalismi.it*, 8/2021, p. 210.

[208] Cfr. il capitolo IV, § 4.3.

[209] Cfr. A. Cabiale, *I limiti alla prova nella procedura penale europea*, cit., p. 250.
La direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3.4.2014 è stata recepita in Italia con d.lgs. 21 giugno 2017, n. 108 (GU Serie Generale n.162 del 13.7.2017), entrato in vigore in data 28.7.2017: il decreto risulta complessivamente fedele al testo della direttiva. Parte della dottrina ha definito tale normativa una «mera opera di unificazione normativa, volta ad assorbire

procedura penale, in tema di estradizione e di rapporti con le autorità giurisdizionali estere[210]. Perciò, oggi l'acquisizione della prova digitale all'estero può effettuarsi tramite due differenti strumenti: la rogatoria e l'ordine europeo di indagine. Come noto, il primo istituto consiste in un meccanismo tramite il quale si chiede che atti destinati ad avere effetti in un procedimento penale in corso in un determinato Stato, vengano effettuati sul territorio di un altro Stato estero, con il consenso di quest'ultimo e ad opera degli organi del medesimo[211]. A tal proposito, l'art. 729 c.p.p., come riformato nel 2017, afferma che «nei casi in cui lo Stato estero abbia posto condizioni all'utilizzabilità degli atti richiesti, l'autorità giudiziaria è vincolata al rispetto di tali condizioni. Se lo Stato dà esecuzione alla richiesta di assistenza con modalità diverse da quelle indicate dall'autorità giudiziaria ai sensi dell'art. 727, co. 9, gli atti compiuti sono inutilizzabili solo nei casi in cui l'inutilizzabilità sia prevista dalla legge (…)». Ne consegue che, solamente nel caso in cui l'eventuale scostamento della condotta tenuta dall'autorità straniera durante l'acquisizione di un modello elettronico sia sanzionato in Italia con l'inutilizzabilità, tale dato non potrà essere posto a fondamento della decisione, non essendo permesso il suo ingresso in sede dibattimentale[212].

---

le Convenzioni di assistenza giudiziaria del 1959 e del 2000, nonché quella "di applicazione dell'accordo di Shengen", oltre alle decisioni quadro 2003/577/GAI sull'esecuzione dei "provvedimenti di blocco dei beni o di sequestro" e 2008/978/GAI in tema di "mandato europeo di ricerca delle prove (MER)"». A. Cabiale, *I limiti alla prova nella procedura penale europea,* cit., p. 250. Peraltro, giova ricordare che quest'ultimo strumento non sarà oggetto della presente trattazione in quanto all'art. 4, c. 2 ha previsto espressamente che «il MER non è emesso allo scopo di richiedere all'autorità di esecuzione di: (…) b) procedere ad accertamenti corporali o prelevare materiale biologico o dati biometrici direttamente dal corpo di una persona, ivi compresi campioni di DNA o impronte digitali». Ne consegue l'esclusione dalla disciplina anche dei modelli elettronici dei relativi dati sopra citati. Per un approfondimento sulla disciplina in generale dell'OEI v. M. Caianiello, *Verso l'attuazione della Direttiva UE sull'Ordine europeo d'indagine penale*, in AA.VV., *Indagini penali e amministrative in materia di frodi IVA e doganali. L'impatto dell'*European Investigation Order *sulla cooperazione transnazionale*, (a cura di) A. Di Pietro, M. Caianiello, Cacucci, Bari, 2016, pp. 305 e ss., M. Daniele, *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale*, in *Dir. pen. cont. –Riv. trim*., 2015, n. 4, pp. 86 e ss., L. Lupária, *Note conclusive nell'orizzonte d'attuazione dell'Ordine europeo di indagine*, in AA.VV., *L'ordine europeo di indagine. Criticità e prospettive*, (a cura di) T. Bene, L. Lupária, L. Marafioti, Giappichelli, Torino, 2016, pp. 249 s., A. Scalfati, *Note minime su cooperazione investigativa e mutuo riconoscimento*, in *Proc. pen. giust*., 2017, pp. 217 e ss., F. Siracusano, *Tra semplificazione e ibridismo: insidie e aporie dell'Ordine europeo di indagine penale*, in *Arch. pen.*, 2017, n. 2, L. Camaldo, *La direttiva sull'ordine europeo di indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione*, in *Dir. pen. cont*., 27.5.2014, M. Daniele, *L'ordine europeo di indagine penale entra a regime: prime riflessioni sul d. lgs. n. 108 del 2017*, in *Dir. Pen. Cont*., 7-8/2017, pp. 208 e ss., M. Caianiello, *L'OEI dalla direttiva al decreto n. 108 del 2017*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017*, (a cura di) M. Daniele, R.E. Kostoris, Giappichelli, Torino, 2018, p. 22, P. Spagnolo, *La nuova cooperazione giudiziaria penale: mutuo riconoscimento e tutela dei diritti fondamentali*, in *Cass. pen*., fasc.3, 1.3.2020, p. 1290.

[210] «La disciplina della cooperazione giudiziaria internazionale, grazie a questi recenti interventi normativi, ha subito notevoli mutamenti, realizzando un nuovo equilibrio tra l'esigenza di favorire la collaborazione fra gli Stati e l'esigenza di garantire il rispetto dei principi fondamentali in tema di giusto processo, in particolare in ordine al tema dell'invalidità nell'acquisizione della prova». A. Colaiocco, *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria*, in *Arch. Pen*., fasc. 1, 2019.

[211] Cfr. M. Chiavario, *Diritto processuale penale*, cit., p. 1262.

[212] Cfr. A. Colaiocco, *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria*, cit.

Venendo al secondo strumento menzionato, l'OEI, esso consiste invece in una decisione giudiziaria emessa o convalidata da un'autorità competente di uno Stato membro ("Stato di emissione"), affinché siano compiuti uno o più atti di indagine specifici in un altro Stato membro ("Stato di esecuzione"), ai fini dell'acquisizione di prove in ambito penale e, quindi anche delle prove digitali[213]. Per vero, seppur l'OEI si ponga rispetto alla Convenzione di Budapest del 2001 in una posizione di preminenza[214], in relazione agli strumenti non espressamente indicati nella suddetta direttiva continuerebbero a trovare applicazione le regole Convenzionali. Pertanto, a partire dal 2.5.2017, anche la raccolta transnazionale della prova digitale fra Stati membri è realizzata attraverso tale strumento in ossequio al tradizionale principio del mutuo riconoscimento ai sensi dell'art. 82 TFUE. Nella prospettiva che qui interessa, la direttiva, pur ribadendo la natura fondamentale del diritto alla protezione dei dati personali[215] e sottolineando un rigoroso rispetto del principio di proporzionalità qualora il trattamento di tali informazioni si renda necessario[216], non sembra aver conferito adeguato risalto al tema della raccolta transnazionale della prova digitale. La norma di riferimento ai fini che qui interessano sembra individuabile nell'articolo 33 del decreto attuativo, il quale - al primo comma - statuisce che «l'autorità giudiziaria che ha emesso l'ordine europeo di indagine concorda con l'autorità di esecuzione le modalità di compimento dell'atto d'indagine o di prova, specificamente indicando i diritti e le facoltà riconosciuti dalla legge alle parti e ai loro difensori». Viene dunque lasciata ampia discrezionalità in ordine alle precise modalità di esecuzione delle operazioni di trattamento di dati biometrici digitalizzati, richiedendo di tenere conto delle procedure e dei protocolli adottati nell'ordinamento interno[217]. Si condivide, inoltre, la posizione della dottrina che, sulla base di un'interpretazione sistematica degli artt. 1 e 33 del d.lgs. 108/2017, ritiene di competenza dell'autorità di emissione dell'OEI la richiesta espressa all'autorità di esecuzione di adottare le modalità previste dalla *lex fori* a pena di inutilizzabilità[218]. Ne consegue un'efficacia extraterritoriale della *lex fori*. In tal senso, l'art. 28 del decreto ha espressamente stabilito che «contro l'ordine di indagine avente ad oggetto il sequestro a fini di prova, la persona sottoposta alle indagini o l'imputato, il suo difensore, la persona alla quale la prova o il bene sono stati sequestrati e quella che avrebbe diritto alla loro

[213] L'autorità di emissione può emettere un OEI solamente quando ritiene soddisfatte le seguenti condizioni: l'emissione dell'OEI è necessaria e proporzionata ai fini del procedimento, tenendo conto dei diritti della persona sottoposta a indagini o imputata; l'atto o gli atti di indagine richiesti nell'OEI avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo (art. 6).

[214] V. il considerando n. 35.

[215] V. il considerando n. 40.

[216] V. il considerando n. 42.

[217] Cfr. M. Daniele, *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale,* in *Dir.pen.cont.*, 4/2015, p. 2 afferma che: «lo scenario di fondo è sempre quello – di tipo orizzontale e non verticale – per cui ciascuno Stato mantiene il proprio diritto delle prove e in questa prospettiva la direttiva ripropone alcune soluzioni già sperimentate in precedenza».

[218] Cfr. M. Daniele, *L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul d. lgs. n. 108 del 2017*, in *Dir. Pen. Cont.*, 7-8/2017, p. 213.

restituzione, possono proporre richiesta di riesame ai sensi dell'articolo 324 del codice di procedura penale». In altre parole, con riferimento all'OEI si nota un certo equilibrio riguardo all'applicabilità delle due normative (*lex fori* e *lex loci*) alle operazioni di acquisizione della *digital evidence*. La struttura dell'OEI permette, seppur con dei limiti[219], di applicare anche in altri Stati membri la *lex fori*[220].

Giova ricordare che è possibile ricorrere all'OEI anche per le operazioni di intercettazione di comunicazioni (artt. 30 e 31). In tal caso, l'OEI deve contenere espressamente le informazioni necessarie ai fini dell'identificazione della persona sottoposta all'intercettazione, la durata auspicata dell'intercettazione, sufficienti dati tecnici, in particolare gli elementi di identificazione dell'obiettivo, per assicurare che l'OEI possa essere eseguito[221]. Ne consegue che, dovendo già essere specificata l'identità del soggetto da intercettare, non si potrà procedere ad un riconoscimento informale da parte della polizia giudiziaria del tipo di quelli descritti nel § 1.4.1. In ogni caso, qualora i requisiti di ammissibilità previsti dalla legge italiana non fossero rispettati, i risultati degli atti istruttori compiuti dovrebbero essere dichiarati inutilizzabili. Tale divieto probatorio, pur non espressamente previsto, può ritenersi implicito nella direttiva, in quanto ricollegabile ad un'inequivocabile scelta del legislatore eurounitario[222].

Con particolare riferimento poi alle regole di ammissibilità delle prove, vigenti nello Stato di esecuzione, l'art. 10 par. 1 lett. *b*) della direttiva prescrive che, se l'OEI concerne un atto "coercitivo"[223], quest'ultimo dev'essere "disponibile in un caso interno analogo", rispetto al diritto del Paese ospitante. Sembrerebbe che, anche con riferimento alle rappresentazioni digitalizzate di dati biometrici grezzi così raccolti, debbano essere presenti tutti i requisiti di ammissibilità della prova digitale previsti dalla normativa interna dello Stato di esecuzione[224]. A tal proposito, l'art. 9 co. 1 e 3

[219] Da una parte, l'autorità di emissione è tenuta ad indicare in modo dettagliato le forme e i protocolli da seguire per evitare che la prova sia inutilizzabile nell'ordinamento di destinazione. Dall'altra, è necessario che l'autorità di esecuzione adatti il proprio *modus operandi* alle forme processuali e operative indicate dallo Stato di emissione, salvo il caso in cui tale richiesta si ponga in contrasto con i principi fondamentali del proprio ordinamento. In tal caso, sarebbe fondamentale capire cosa rientra nel concetto di principio fondamentale: di sicuro si ricomprende il rispetto della libertà morale delle persone che partecipano al processo. Più incerto se ricomprenda anche la necessità di osservare le garanzie difensive e il metodo dell'esame incrociato.

[220] Cfr. M. Daniele, *L'ordine europeo di indagine penale entra a regime*, cit., p. 70.

[221] Riguardo, più specificamente, alle intercettazioni relative a dispositivi o sistemi informatici che si trovino all'estero, gli artt. 43 e 44 del d.lgs. 108/2017 indicano unicamente il pubblico ministero quale organo competente all'emissione dell'OEI, trascurando il fatto che l'art. 267 c.p.p. postula, a livello interno, l'autorizzazione del giudice per le indagini preliminari. Peraltro, manca un espresso richiamo alle ulteriori condizioni di ammissibilità delle intercettazioni previste dalla legge italiana. Rimane fermo che la relazione illustrativa al decreto apprestata dal Governo dà per scontato che l'OEI possa essere emesso «alle condizioni stabilite dalla legge italiana, così scongiurando ogni pericolo che si vogliano aggirare» e nei «limiti o vincoli posti dal diritto interno».

[222] Cfr. A. Colaiocco, *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria*, cit.

[223] Ossia tale da interferire con i diritti fondamentali: v. il considerando n. 16.

[224] Qualora questi non fossero osservati, l'acquisizione probatoria rischierebbe di entrare in conflitto con i diritti fondamentali, in tal senso compressi in modo del tutto arbitrario. Sul punto v. C. Edu, *Zakharov c. Russia*, 4.12.2015, 227 s.

del decreto attuativo prescrive che l'OEI vada rifiutato se «non ricorrono i presupposti che la legge italiana impone» per il compimento dell'atto istruttorio richiesto, e non è possibile compiere altri atti «comunque idonei al raggiungimento del medesimo scopo»[225].

Dalla disciplina in generale sembra pertanto potersi intravedere la *ratio* di fondo: ogni deviazione rispetto agli standard di acquisizione della prova previsti dal diritto nazionale deve risultare assolutamente necessaria, dovendo trovare una conferente motivazione nelle peculiarità della singola situazione concreta[226]. In particolare, sia nel caso di rogatoria internazionale, sia nel caso di ordine europeo d'indagine, le *best practices* previste per l'acquisizione della *digital evidence* nell'ordinamento interno (cfr. il § 1.2) assumono una rilevanza fondamentale anche per la raccolta transfrontaliera della stessa. Pertanto, analogamente a quanto detto per la *digital evidence tout court*, sembra che il rispetto delle linee-guida per la raccolta e l'acquisizione dei dati biometrici digitalizzati costituisca un canone ormai ineludibile per una corretta acquisizione processuale degli stessi.

1.5.1.4. La proposta di regolamento sugli ordini di produzione e conservazione di prove elettroniche 2018/0108 (COD)

Come visto poc'anzi, sia l'ordine europeo di indagine, sia lo strumento della rogatoria internazionale non disciplinano espressamente l'acquisizione di prove digitali. Infatti, più che per queste ultime tipologie di elementi di prova, i due strumenti sembrano essere stati concepiti per le prove materiali[227]. Invero, per funzionare al meglio, la rogatoria e l'OEI presuppongono la possibilità di individuare un unico Stato di esecuzione, il quale, peraltro, deve attenersi alle formalità e procedure previste in base alla *lex fori*, salvo il caso in cui non siano *compliant* con i principi fondamentali della *lex loci* (cfr. *supra* il § 1.5.1)[228].

---

[225] V. su questo punto anche A. Cabiale, *I limiti alla prova nella procedura penale europea*, cit., p. 159.

[226] La medesima *ratio* sembrerebbe guidare altresì l'esecuzione delle attività di indagine atipiche qualora lo Stato di esecuzione dovesse constatare l'assenza nel proprio diritto di una previsione normativa nazionale che regoli l'esecuzione di un determinato atto. In questo caso non è chiaro a quale disposizione della direttiva occorra fare riferimento. L'art. 11 par. 1 lett. *f*) della direttiva permette di rifiutare l'esecuzione dell'ordine qualora l'attività oggetto di richiesta risulti incompatibile con l'articolo 6 TUE. L'art. 9 lett. *d*) del d.lgs. 108/2017 stabilisce poi che, nel caso in cui l'atto non sia previsto dalla legge italiana, deve procedersi in ogni caso al compimento di «tutti gli atti di indagine che non incidono sulla libertà personale e sul diritto all'inviolabilità del domicilio». Per un approfondimento sul punto v. F. Nicolicchia, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, cit., pp. 190 e ss.

[227] Cfr. sul punto M. Daniele, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Rev. Bras. de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, 2019, p. 1280 e F. Galli, *Information Sharing as a Tool in the Fight against Impunity in the European Union*, in AA.VV., *The Fight Against Impunity in EU Law*, (a cura di) L. Marin, S. Montaldo, Hart Publishing, New York, 2020, pp. 172-173.

[228] Si conviene con M. Daniele, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1281: «tale condizione – non esente da margini di ambiguità – se non altro mira ad evitare che le modalità di raccolta delle prove si appiattiscano su una *lex fori* non sufficientemente attenta alle garanzie, dando spazio ai superiori standard di tutela eventualmente previsti dalla *lex loci*, in una logica di contemperamento della sovranità dello Stato richiedente con quella dello Stato di esecuzione».

Per vero, la principale motivazione che ha portato alla presentazione di una più specifica proposta di regolamento sul tema, è stata - per certi versi - la rilevante difficoltà, a fronte di una molteplicità di Stati a cui sarebbe possibile rivolgere la richiesta istruttoria, di individuare un unico Stato di esecuzione[229]. Infatti, considerata la peculiare dispersione delle prove digitali (cfr. il § 1.1)[230], risultano potenzialmente plausibili molteplici *leges loci*: dallo Stato in cui opera o ha sede legale il *service provider*, allo Stato in cui si trova fisicamente il *server* ove le prove risultino reperibili. Ne è conseguito il sorgere di un concreto pericolo di individuazione arbitraria dello Stato competente ad operare. Per certi versi, viene a mente il meccanismo previsto dall'art. 234 *bis* c.p.p., così come trasposto dall'art. 32 della Convenzione di Budapest nel nostro sistema interno, il quale prescrive che «è sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare». Senonché in questo modo, ciascuna azienda stabilisce di volta in volta, sulla base dei propri interessi, se ed entro quali limiti cooperare. Tale contesto di incertezza normativa ha dunque spinto la Commissione Europea a depositare una prima proposta di *regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* ("proposta della Commissione")[231], ad oggi ancora in fase di negoziazione. Più nel dettaglio, tale bozza «affronta il problema specifico della natura volatile delle prove elettroniche e della loro dimensione internazionale. Essa mira ad adattare i meccanismi di cooperazione all'era

[229] Oltre a questo aspetto, bisogna tenere conto del fatto che, come accennato *supra* al § 1.2, alcune associazioni e forze di polizia hanno sviluppato in ambito internazionale le proprie linee guida. Questo può creare alcuni problemi nella cooperazione fra gli Stati qualora vengano commessi reati transnazionali, dal momento che le *digital evidences* acquisite in un paese potrebbero dover essere presentate davanti a tribunali di un altro. Le prove alterate potrebbero essere state acquisite senza il livello di sicurezza richiesto e potrebbero essere giuridicamente inammissibili. V. sul punto, G. Costabile, *Digital forensics & digital investigation: classificazione, tecniche e linee guida nazionali ed internazionali*, AA.VV., Cyber forensics *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, (a cura di) S. Aterno, F. Cajani, G. Costabile, D. Curtotti, Giappichelli, Torino, 2021, p. 9, F. Galli, *Information Sharing as a Tool in the Fight against Impunity in the European Union*, in AA.VV., *The Fight Against Impunity in EU Law*, (a cura di) L. Marin e S. Montaldo, Hart Publishing, New York, 2020, pp. 177 e 189, M. Böse, *An Assessment of the Commission's Proposal on Electronic Evidence*, reperibile all'inidirizzo https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf (visualizzato in data 18.5.2021).

[230] Giova ricordare che «nell'ultimo decennio, il numero dei reati che coinvolgono computer e Internet è cresciuto, stimolando un aumento delle aziende e dei prodotti che mirano a supportare le forze dell'ordine nella ricerca delle prove digitali per determinare i perpetratori, i metodi, i tempi e le vittime del crimine informatico». G. Costabile, *Le indagini digitali*, in AA.VV., Cyber forensics *e indagini digitali*, cit., p. 68.

[231] "*Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*" del 17 aprile 2018 (COM(2018) 225 final). Reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52018PC0225 (visualizzato in data 18.5.2021). S'intende dare conto anche del fatto che, contestualmente alla presentazione della bozza di regolamento, la Commissione europea ha pubblicato altresì una Proposta *for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings* COM/2018/226 final - 2018/0107 (COD), reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN (visualizzato in data 18.5.2021). Per una puntuale ricostruzione sul tema v. *ex multis* O. Calavita, *La proposta di regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, in *www.lalegislazionepenale.it*, 30.3.2021.

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 (…). Essa inoltre rende più rapido il processo per assicurare ed ottenere prove elettroniche conservate e/o detenute da prestatori di servizi stabiliti in un'altra giurisdizione»[232]. Quindi, mentre la direttiva OEI regola qualsiasi atto d'indagine, concernente anche i dati digitali, ma senza dettare specifiche disposizioni su questa particolare tipologia di evidenza, la proposta di regolamento fornisce alle autorità un ulteriore strumento senza sostituire le disposizioni della direttiva 2014/41. Infatti, dal momento che l'acquisizione di prove elettroniche presenta problematiche specifiche che non riguardano gli altri atti d'indagine contemplati dalla direttiva OEI, anziché procedere con una modifica di quest'ultima, si è deciso di creare uno strumento a sé stante. Al fine di agevolare il più possibile la raccolta di prove elettroniche, il nuovo strumento di cooperazione giudiziaria si baserà su principi di reciproco riconoscimento[233].

In primis, la novità strutturale che balza subito agli occhi degli interpreti consiste nella scelta di procedere tramite regolamento, anziché con direttiva[234]: questa opzione viene giustificata nella relazione introduttiva ove si afferma che «la proposta riguarda procedure transfrontaliere, per le quali sono necessarie norme uniformi» e pertanto «non occorre lasciare un margine agli Stati membri per recepirle»[235].

---

[232] "*Proposta di regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*" (COM/2018/225 final - 2018/0108 (COD) disponibile su https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52018PC0225 (ultimo accesso in data 13.4.2021).

[233] «Ai fini della notifica e dell'esecuzione dell'ordine non occorrerà coinvolgere direttamente l'autorità del paese in cui si trova il destinatario dell'ordine, tranne se il destinatario non vi ottempera spontaneamente, nel qual caso l'ordine sarà fatto eseguire e sarà necessario l'intervento dell'autorità competente del paese in cui si trova il rappresentante. Lo strumento richiede pertanto una serie di solide garanzie e disposizioni, come la convalida da parte di un'autorità giudiziaria in ogni singolo caso. Ad esempio, l'ordine europeo di produzione riguardante dati relativi alle operazioni o al contenuto (ma non dati relativi agli abbonati o agli accessi) può essere emesso solo per reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno 3 anni o per specifici reati contro la sicurezza cibernetica, favoriti dall'uso del ciberspazio o connessi al terrorismo, specificati nella proposta». *Relazione della Proposta di Regolamento,* cit., disponibile su https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52018PC0225 (ultimo accesso in data 13.4.2021).

[234] Si conviene con A. Rosanò, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione europea: le proposte della commissione europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence),* in *www.lalegislazionepenale.it,* 16.10.2020 che si tratti «di una scelta – politica, prima ancora che giuridica – di non poco conto se si considera la storia della cooperazione giudiziaria in materia penale».
Ciò nonostante, la base giuridica rimane sempre l'art. 82, par. 1 TFUE, v. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:C:2016:202:TOC (visualizzato in data 14.4.2021).

[235] *Proposta di regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* (COM/2018/225 final - 2018/0108 (COD) disponibile su https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52018PC0225 (ultimo accesso in data 13.4.2021), p. 6. Sul punto v. R. M. Geraci, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento E-evidence*, in *Cass. pen*., 2019, p. 1342, A. Cabiale, *I limiti alla prova nella procedura penale europea*, cit., p. 272 e O. Calavita, *La proposta di regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto,* in *www.lalegislazionepenale.it,* 30.3.2021.

Quanto al funzionamento, in estrema sintesi, la proposta di regolamento contempla due ordini emanabili: quello di "conservazione", disposto dall'autorità giudiziaria inquirente direttamente nei confronti del prestatore di servizi del sistema informatico o telematico, localizzato in un altro Stato, al quale detta autorità ordina la conservazione di prove elettroniche; un successivo ordine di "produzione", ossia «la decisione vincolante di un'autorità di emissione di uno Stato membro che ingiunge a un prestatore di servizi che offre servizi nell'Unione (…) di produrre prove elettroniche»[236]. Più nel dettaglio, l'OCE è caratterizzato da una struttura particolarmente snella che non richiede alcun intervento giurisdizionale necessario[237] e permette di congelare i dati richiesti per un periodo massimo di 60 giorni. Per l'OPE, invece, sono stati previsti termini più stringenti e i suoi contenuti necessitano della validazione da parte di un giudice: generalmente la produzione deve avvenire entro 10 giorni dall'emissione dell'ordine o, in casi di urgenza, entro 6 ore[238].

Con riferimento ad alcune caratteristiche del nuovo atto, riecheggia la disciplina dell'OEI: così, la misura dovrà essere "necessaria", "proporzionata" e in determinati casi la sua emissione sarà condizionata dalla gravità del reato perseguito. Gli ordini emessi sono trasmessi tramite appositi certificati (EPOC-CR e EPOC), il cui scopo è quello di «fornire tutte le informazioni necessarie al destinatario in un formato standardizzato, escludendo dati sensibili contenuti negli ordini di produzione e di conservazione come quelli relativi alla necessità o alla proporzionalità di tali provvedimenti investigativi, per evitare di compromettere la segretezza e il buon esito delle indagini»[239].

Si ritiene che la novità strutturale più rilevante abbia ad oggetto il destinatario degli ordini, che non è un'autorità giudiziaria dello Stato di esecuzione, ma - direttamente - il legale rappresentante dei *service provider*[240] designato dal prestatore di servizi oppure, in mancanza, o in caso di inadempimento

---

[236] Art. 2, nn. 1 e 2. Per approfondimenti sul funzionamento v. R. M. Geraci, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento E-evidence*, in *Cass. pen*., 2019, p. 1340, M. Gialuz, J. Della Torre, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir.pen.cont*., 2018, fasc. 5, pp. 277 e ss., A. Rosanò, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'unione europea: le proposte della commissione europea sugli ordini di produzione e conservazione di prove elettroniche* (*e-evidence*), in *www.lalegislazionepenale.it*, 16.10.2020.

[237] L'OCE viene emesso anche da un pubblico ministero senza che sia prevista una necessaria convalida postuma da parte dell'autorità giudiziaria.

[238] Un'altra differenza riguarda il fatto che gli ordini di produzione possono essere emessi solo se la normativa interna preveda una misura della stessa tipologia in un caso interno analogo (art. 5, par. 2), mentre gli OCE potranno essere adottati in relazione a qualsiasi reato (art. 6, par. 2).

[239] Cfr. R. Pezzuto, *Accesso transazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione Europea al vaglio del Consiglio dell'Unione*, in *Dir. Pen. cont*, fasc. 2/2019, p. 80.

[240] Per "prestatore di servizi", s'intende in base all'art. 2 par. 3 «la persona fisica o giuridica che fornisce una serie determinata di servizi». Tra questi si annoverano: 1) i servizi di comunicazione elettronica come definiti dalla direttiva che istituisce il codice delle comunicazioni europeo, nei quali vanno annoverate le comunicazioni *Voice over IP* (VoIP), la messaggistica istantanea e i servizi di posta elettronica; 2) i servizi della società dell'informazione per i quali la conservazione dei dati è una componente propria del servizio fornito dall'utente, tra cui i social network, i mercati online che agevolano le operazioni tra utenti e altri prestatori di servizi *hosting*; 3) i servizi di nomi di dominio internet e di numerazione IP, quali i prestatori di indirizzi IP, i registri

dello stesso, un qualsiasi stabilimento del prestatore di servizi presente all'interno dello spazio di sicurezza, libertà e giustizia[241]. Tale soggetto ricevente è poi tenuto eventualmente ad informare l'autorità di emissione che l'ordine è «incompleto o contiene errori manifesti o informazioni insufficienti per eseguirlo», ovvero che non è stato possibile «ottemperare (…) a causa di forza maggiore o per impossibilità materiale»[242]. Solo nel caso dell'ordine di produzione, colui che detiene la prova ha anche la possibilità di rifiutare l'esecuzione qualora ritenga la sussistenza di una manifesta violazione della Carta dei diritti fondamentali dell'Unione europea o gli risulti che la richiesta sia manifestamente arbitraria[243]. A questo punto, l'autorità dello Stato di esecuzione viene coinvolta solo nel caso in cui il prestatore non adempia e chi ha emesso l'ordine intenda persistere con la richiesta[244]. Rimane fermo che i destinatari degli ordini sono tenuti a garantire la riservatezza dei dati prodotti o conservati e, su richiesta espressa dell'autorità emittente, devono astenersi dal rivelare al soggetto interessato l'intento di conservare o trasmettere i dati digitali richiesti, al fine di non ostacolare il corretto corso del procedimento penale[245].

Quanto ai dati richiedibili, la proposta della Commissione ne prevede quattro tipologie[246]: da una parte, i dati relativi agli abbonati alla piattaforma e agli accessi, considerati dalla proposta di regolamento meno invasivi della sfera del singolo, dall'altra, i dati relativi ai contenuti e alle operazioni[247]. I primi sono quelli che riguardano l'identità di un soggetto abbonato (*subscriber data*), nonché il tipo di servizio e la sua durata, compresi quindi i dati tecnici, fatta eccezione delle password[248]; i dati relativi agli accessi (*access data*), invece, costituiscono una categoria inedita e

---

di nomi di dominio, i *registrar* di nomi di dominio e i connessi servizi per la *privacy* o *proxy*. Esulano, invece, dall'applicazione del regolamento i servizi della società dell'informazione per i quali «la conservazione dei dati non è una componente propria del servizio fornito all'utente bensì un elemento puramente accessorio, quali i servizi giuridici, architettonici, ingegneristici e contabili forniti online o a distanza»[240]. Cfr. il considerando n.16. Su questo punto si v. F. Galli, *Information Sharing as a Tool in the Fight against Impunity in the European Union*, cit., p. 172.

[241] Cfr. l'art. 7.

[242] Cfr. l'art. 9 parr. 3 e 4 e art. 10 parr. 4 e 5.

[243] Cfr. l'art. 9, par. 5, co. 2.

[244] Cfr. l'art. 14.

[245] Cfr. su questo punto O. Calavita, *La proposta di regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, in *www.lalegislazionepenale.it*, 30.3.2021.

[246] «[…] *it aims to include internet access services, 'internet-based services enabling inter-personal communications such as Voice over IP, instant messaging and e-mail services', as well as 'cloud and other hosting services' and 'digital marketplaces', and the providers of online services and platforms such as Skype, WhatsApp, Telegram, Dropbox and eBay would also be covered. Providers of internet domain names and IP numbering services are relevant because they 'can provide traces allowing for the identification of an individual or entity involved in criminal activity'*». F. Galli, *Information Sharing as a Tool in the Fight against Impunity in the European Union*, cit. p. 176.

[247] «Il presente regolamento disciplina l'acquisizione solo dei dati conservati, ossia dei dati detenuti dal prestatore di servizi al momento della ricezione di un certificato di ordine europeo di produzione o di conservazione. Non impone un obbligo generale di conservare i dati né autorizza l'intercettazione di dati o l'ottenimento di dati che saranno conservati dopo la ricezione del certificato di ordine di produzione o di conservazione. I dati devono essere forniti a prescindere dal fatto che siano criptati o meno». Cfr. il considerando n. 19.

[248] Cfr. l'art. 2, par. 7.

hanno lo scopo di identificare un soggetto mediante il ricorso a *file di log-in* (connessione) e di *log-off* (disconnessione)[249].

Ben più invasiva è la disposizione che consente di utilizzare lo strumento in esame per i dati relativi alle operazioni (*transactional data*) e al contenuto (*content data*), consentendo, in questo modo, di "sorvegliare" e ricostruire potenzialmente anche gli aspetti più intimi del soggetto i cui dati sono richiesti. Tra queste ultime due tipologie di informazioni, risultano di particolare rilievo - ai fini della presente ricerca - i dati relativi al contenuto, i quali comprendono una gamma eterogenea e residuale di informazioni acquisibili, riferibili a qualsiasi dato conservato in formato digitale, come testo, voce, video, immagine o suono. Ne consegue che, tra questi, possano ragionevolmente annoverarsi - in via esegetica - i dati biometrici digitalizzati suscettibili di confronti con altri[250]. Proprio in ragione dell'oscurità dei contorni della tipologia di dati richiedibili, però, sia l'*European Data Protection Supervisor* (EDPS)[251] sia la dottrina[252], hanno posto in luce l'esigenza che il regolamento adotti una definizione più precisa, al fine di scongiurare il rischio di addossare al prestatore di servizi il compito di stabilire se i dati richiesti siano annoverabili effettivamente nelle categorie disciplinate oppure no. Si ritiene opportuno specificare, poi, che tali dati devono essere già in possesso del *service provider*: all'autorità di emissione non è consentito infatti di imporre al prestatore di servizi il reperimento di ulteriori dati in relazione ai quali non vanti alcun obbligo o che non siano ancora stati registrati, così come non sono contemplate le intercettazioni in tempo reale dei flussi informatici o telematici.

Peraltro è previsto un ulteriore presupposto legittimante l'emissione di ordini: mentre gli OCE e gli OPE riguardanti gli accessi e gli abbonati possono essere emessi per qualsiasi tipo di reato, gli OPE riguardanti i contenuti e le operazioni possono essere emessi solo per alcune tipologie di reato normativamente previste (sintomatico il caso della pornografia minorile) oppure per reati puniti con pena detentiva pari, nel massimo, ad almeno tre anni (che tuttavia nell'ordinamento italiano sanziona anche reati di ridotto allarme sociale, rendendo molto ampio il campo di applicazione anche di questa tipologia di OPE)[253].

---

[249] Cfr. il considerando n. 21.

[250] In tal senso, secondo parte della dottrina l'elencazione delle tipologie di dati parrebbe meramente esemplificativa e non tassativa. Cfr. A. Rosanò, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione Europea: le proposte della Commissione europea sugli ordini di produzione e conservazione di prove elettroniche* (*e-evidence*), in *www.lalegislazionepenale.it*, 16.10.2020, p. 16.

[251] EDPS, *Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters*, n. 7/2019, Bruxelles, 06 novembre 2019, disponibile sul sito https://edps.europa.eu/sites/edp/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf (visualizzato in data 14.4.2021).

[252] Cfr. A. Rosanò, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione Europea: le proposte della Commissione europea sugli ordini di produzione e conservazione di prove elettroniche* (*e-evidence*), in *www.lalegislazionepenale.it*, 16.10.2020, p. 16.

[253] Cfr. O. Calavita, *La proposta di regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit.

Come noto, la proposta della Commissione è già stata oggetto di ampie discussioni in seno al Consiglio dell'Unione Europea e al Parlamento, i quali hanno presentato talune proposte emendative del progetto iniziale[254].

Partendo dal Consiglio, esso ha proposto una serie di modifiche piuttosto rilevanti, tra le quali giova richiamare, per i fini della presente ricerca, un ben più ampio contesto applicativo del regolamento, di cui si propone l'estensione anche alla fase di esecuzione di pene detentive, nel caso in cui il condannato si sia sottratto alla giustizia. Particolarmente interessante, poi, è l'idea di introdurre la possibilità di accesso agli ordini non solo per l'identificazione dell'indagato o imputato, ovvero per l'acquisizione di materiale probatorio, ma anche per l'individuazione del soggetto condannato, non in contumacia, latitante che deve scontare una pena o una misura di sicurezza privative della libertà della durata di almeno 4 mesi[255]. Rispetto a tale proposta emendativa, si ritengono direttamente interessati tutti quei dati biometrici in formato elettronico in grado di eseguire, tramite una comparazione con altri dati, il riconoscimento della persona.

Quanto alla procedura di emissione degli ordini, si prevede che in casi di urgenza debitamente giustificati (art. 4, par. 5), sia consentita la trasmissione da parte delle autorità destinatarie degli ordini dell'EPOC-PR e dell'EPOC riguardante i dati relativi agli accessi e agli abbonati al destinatario in assenza di una convalida formale da parte dell'autorità giudiziaria, che dovrà comunque essere oggetto di un'apposita richiesta entro 48 ore. Nel caso di rifiuto, l'autorità di emissione è tenuta a revocare l'ordine ed eliminare i dati eventualmente trasmessigli *medio tempore*. Con riferimento ai dati concernenti le operazioni, se questi appartengono a una persona non residente nel territorio dello Stato di emissione e vi è il dubbio che possano essere oggetto di protezione nello Stato di esecuzione (perché magari coperti da immunità, privilegi, norme a tutela della libertà di stampa etc.), sono previste due procedure - una preventiva e una successiva - di consultazione con lo Stato di esecuzione (art. 5, par. 7). In tal modo, si fornisce una tutela attenta agli interessi individuali senza frustrare del tutto la necessità dello Stato di raccolta delle prove[256].

Il Consiglio dell'Unione europea ha poi introdotto un nuovo art. 7 *bis* che regola una procedura di notifica allo Stato di esecuzione qualora lo Stato di emissione intenda richiedere la produzione di dati relativi al contenuto di una persona non residente sul proprio territorio nazionale, aventi natura a tal

---

[254] *Orientamento generale del Consiglio sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* del 6 e 7 dicembre 2018, 2018/0108(COD) e *Progetto di Relazione Sippel sulla proposta* di *regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* del 24 ottobre 2019, COM(2018)0225 – C8-0155/2018 – 2018/0108(COD).

[255] Cfr. gli artt. 3, par. 2, 5 par. 3, e 6 par. 2 dell'orientamento generale.

[256] Cfr. O. Calavita, *La proposta di regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit.

punto sensibile che, per loro tramite, «le persone possono rivelare i propri pensieri e dettagli sensibili della loro vita privata». La notifica viene trasmessa sia al prestatore di servizi[257], sia allo Stato di esecuzione e ha lo scopo di porre in condizione quest'ultimo di comunicare all'autorità di emissione l'eventuale presenza di immunità, privilegi o lesioni di diritti e interessi fondamentali o violazioni delle norme sulla libertà di stampa[258].

Inoltre, l'art. 8 par. 2, così come emendato dal Consiglio dell'Unione europea, sottolinea espressamente che le modalità di trasmissione dei dati debbano essere sicure ed affidabili. Trattasi di una precisazione apprezzabile in quanto ogni modificazione, anche minima, dei dati trasmessi potrebbe causarne l'inutilizzabilità[259]. Stessa *ratio* presenta altresì l'art. 9, par. 1, secondo il quale l'esecuzione dell'EPOC è modificata introducendo un'espressa previsione per mezzo della quale i dati debbano essere trattati secondo «modalità sicure e affidabili che consentano di stabilire l'autenticità e l'integrità» degli stessi[260].

L'art. 12 *ter* sancisce poi il principio di specialità, ossia stabilisce un divieto di utilizzabilità dei dati ottenuti in procedimenti diversi da quelli per i quali si procede[261]. In questo modo, si evitano potenziali strumentalizzazioni di nuovi ordini o utilizzazioni abusive di dati raccolti.

Con riferimento ai rimedi, la nuova formulazione dell'art. 17 prevede che entrambi gli OCE e gli OPE siano reclamabili dai soggetti interessati, dal momento che il ricorso giurisdizionale, ai sensi del diritto interno, è usufruibile da «qualsiasi persona i cui dati sono stati ricercati»[262].

---

[257] Peraltro, a mutare sarebbe anche la definizione di "prestatore di servizi", coincidente con coloro che offrono la possibilità agli utenti di comunicare tra loro oppure che trattano dati per conto degli utenti (art. 2, par. 3). Più nel dettaglio, sono esclusi i servizi finanziari e coloro che offrono la possibilità di comunicare solo con il prestatore di servizi e non tra loro e che non concedono la possibilità di tracciare o conservare i dati.

[258] È espressamente previsto che, al fine di non ritardare l'esecuzione, la notifica allo Stato non abbia effetto sospensivo (art. 7-*bis*, par. 4). Sul punto si conviene con O. Calavita, *La proposta di regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., che ritiene che: «[…] sarebbe più opportuno prevedere una notifica con effetto parzialmente non sospensivo – che obblighi cioè il SP a conservare il dato ma non a produrlo, in attesa della decisione dell'autorità – allo Stato in cui risiede il soggetto nei cui confronti vengono richiesti i dati, che non necessariamente coincide con lo Stato di esecuzione».

[259] Cfr. O. Calavita, *La proposta di regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit.

[260] A tal proposito, giova ricordare la specifica proposta da parte della Commissione europea "e-CODEX" di *regolamento del Parlamento Europeo e del Consiglio relativo a un sistema informatizzato di comunicazione per i procedimenti civili e penali transfrontalieri (sistema e-CODEX) e che modifica il regolamento (UE) 2018/1726*, del 02 dicembre 2020, COM(2020)712, la cui direzione sarà posta in capo all'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA). Tale sistema permetterà lo scambio di messaggi, dati, documenti e informazioni in modo rapido e sicuro, mantenendo integra l'identità digitale del mittente e l'avvenuta ricezione di quanto inviato. Per maggiori informazioni v. https://eur-lex.europa.eu/legal-content/IT/TXT/?qid=1618478788113&uri=CELEX%3A52020SC0541 (visualizzato in data 15.5.2021).

[261] Sono previste due eccezioni: la prima richiama i reati di cui all'art. 5, parr. 3 e 4, mentre la seconda prevede che i dati raccolti possano essere utilizzati al fine di evitare una minaccia grave e immediata per la pubblica sicurezza dello Stato di emissione o i suoi interessi fondamentali (art. 12-*ter*, par. 1).

[262] Cfr. il considerando n. 54. V. F. Galli, *Information Sharing as a Tool in the Fight against Impunity in the European Union*, cit. p. 179.

Infine, riguardo alle sanzioni, l'art. 13, par. 3, stabilisce che la sanzione pecuniaria applicabile dagli Stati membri nei confronti dei *service provider* inadempienti alla richiesta possa ragionevolmente consistere in una somma pari fino al 2% del fatturato complessivo annuo del prestatore di servizi, avendo riguardo alla natura, alla gravità e la durata della violazione, se è stata commessa intenzionalmente o per negligenza, se il fornitore del servizio è stato ritenuto responsabile per analoghe violazioni precedenti e la solidità finanziaria del prestatore di servizi ritenuto responsabile[263].

Dal canto suo, il Parlamento europeo ha assegnato la discussione della proposta alla commissione LIBE (*"Committee on civil liberties, justice and home affairs")* che, in data 24.10.2019, ha presentato un progetto contenente numerose modifiche[264]. La relazione segue la *ratio* di una massima partecipazione agli ordini dello Stato di esecuzione: per tale ragione è stato previsto che la notifica sia dell'EPOC sia dell'EPOC-PR abbia luogo tanto nei confronti del *provider* quanto dello Stato di esecuzione. I motivi di diniego da parte dello Stato di esecuzione nei confronti dell'ordine sono disciplinati nell'art. 10 *bis*[265]: essi concernono essenzialmente questioni di legittimità[266].

Un profilo di particolare interesse è rappresentato dalla previsione di un compendio probatorio minimo affinché l'ordine venga emesso, ossia la cd. *high probability*, avente lo scopo di scongiurare il rischio di indagini preventive e meramente conoscitive. In questo modo, si assicura il rispetto dei principi di proporzionalità e di necessità.

Insomma, è ancora presto per trarre conclusioni sulle sorti di questa proposta. Certamente, rispetto alla direttiva 2014/41 si registra un significativo passo avanti per una più specifica regolamentazione delle *digital evidences*, nell'ottica della cooperazione giudiziaria euro-unitaria in materia penale, senza tuttavia ancora affrontare in modo diretto le peculiarità di un dato biometrico digitalizzato, ma dando comunque una tangibile dimostrazione di un sforzo effettivo nell'enunciazione di principi e disposizioni fondamentali comuni che valgano anche per il trattamento di modelli elettronici.

1.5.2. Le richieste di evidenze digitali ai *service providers* di Paesi extra UE

Simmetricamente alla trattazione dei più rilevanti istituti di cooperazione internazionale, ai fini della presente ricerca, s'intende dar conto, seppur per brevi cenni, della frequente ipotesi in cui

[263] Cfr. il considerando 45 *bis*.

[264] Progetto di Relazione Sippel sulla proposta di *Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* del 24 ottobre 2019, COM(2018)0225 – C8-0155/2018 – 2018/0108(COD).

[265] Cfr. il considerando 42 *ter* della Commissione LIBE.

[266] I motivi di merito potranno essere oggetto di reclamo nello Stato di emissione. Art. 17, paragrafo 3 *bis*, relazione della Commissione LIBE.

l'evidenza digitale sia detenuta proprio da un *service provider*[267] di un Paese extra UE[268]. Infatti, più della metà delle investigazioni penali, secondo i dati raccolti dalla Commissione europea resi pubblici nell'aprile del 2018[269], necessitano di una richiesta di accesso ad una *e-evidence* situata in un SP estero, ma a causa della mancanza o dell'inefficacia dei meccanismi di cooperazione internazionale, «*almost two thirds of crimes involving cross-border access to e-evidence cannot be effectively investigated or prosecuted*»[270]. Il numero è certamente destinato a salire, considerato l'incremento delle richieste di informazioni rivolte dagli Stati membri dell'Unione Europea ai maggiori *service provider* (Google, Facebook, Apple, Microsoft)[271]. Trattasi di piattaforme utilizzate nella quotidianità da un grandissimo numero di utenti per lo scambio di una rilevante quantità di dati e informazioni. Tra questi ultimi, risulta ancora più frequente l'invio e la ricezione di immagini ritraenti volti suscettibili, come già visto *supra* al capitolo I § 3.3, di comparazione con altre immagini digitalizzate a fini di identificazione (cfr. il capitolo I, § 2.2). Ma non solo. La stessa cosa può accadere con il riconoscimento vocale. Si pensi a tutte le volte in cui, anziché inoltrare un messaggio di testo tradizionale, si opta, perché più comodo e più veloce, per inviare un messaggio vocale. Insomma, il tema lambisce anche il trattamento dei dati biometrici a fini di giustizia. A tal proposito, volendo operare una prima macro semplificazione, la regola generale - anche alla luce del recente *Cloud Act*[272] che ha già condotto al

[267] Da qui in avanti "SP".

[268] Su questo tema v. M. Pittiruti, *L'apprensione all'estero della prova digitale*, in AA.VV., *Dimensione tecnologica e prova penale*, (a cura di), L. Luparia, L. Marafioti, G. Paolozzi, Giappichelli, Torino, 2019, pp. 204 e ss. e M. Daniele, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Rev. Bras. de Direito Processual Penal*, 2019, vol. 5, n. 3, pp. 1277-1296.

[269] COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT, *Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, SWD/2018/118 final, reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN (visualizzato in data 13.5.2021).

[270] Cfr. COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT, cit., p. 17.

[271] Cfr. COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT, cit., p. 15. V. sul punto anche L. Freeman, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, in *Fordham International Law Journal*, Vol. 41, Issue 2, pp. 310 e ss.

[272] *Clarifying Lawful Overseas Use of Data Act* (*CLOUD Act*) del 23 marzo 2018, reperibile su https://www.congress.gov/bill/115th-congress/senate-bill/2383/text (visualizzato in data 23.6.2021). La legge ha introdotto significative modifiche allo *Stored Communications Act* del 1986 (reperibile all'indirizzo https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285), affermando che la richiesta di produzione dei dati in possesso dei SP prescinde dal luogo dove sono situati i server. Infatti, è sufficiente che tali *provider* siano subordinati alla sovranità statunitense, e che esercitino il controllo sui dati informatici richiesti, per vincolarli al rispetto della pretesa. E' stata prevista, inoltre, la possibilità di stipulare accordi esecutivi tra Stati esteri e Stati Uniti per consentire ai fornitori di servizi statunitensi di rispondere a determinati ordini stranieri che chiedono accesso ai dati delle comunicazioni. A tal proposito, il Consiglio europeo pare voler sostenere un approccio comune a livello dell'UE e incoraggia la Commissione a proseguire i contatti con le autorità statunitensi e a presentare urgentemente un mandato di negoziato. In data 5 febbraio 2019 si colloca la Raccomandazione della Commissione europea che autorizza l'avvio di negoziati in vista di un accordo tra l'Unione europea e gli Stati Uniti d'America sull'accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale con l'obiettivo di stabilire «norme comuni per affrontare la questione giuridica specifica per l'accesso ai dati relativi al contenuto e a quelli non relativi al contenuto detenuti dai prestatori di servizi nell'Unione europea o negli Stati Uniti» nonché integrare «le proposte dell'UE riguardanti le prove elettroniche

data-sharing agreement USA-UK del 3 ottobre 2019[273] - sembra quasi sempre quella di una richiesta formale di assistenza giudiziaria agli Stati interessati a collaborare[274]. La normativa di riferimento sembra rimanere - per il momento [275]- contenuta negli artt. 31, 33 e 34 della succitata Convenzione di Budapest (ratificata anche dagli USA)[276]. Peraltro, la Convenzione di Budapest lascia ai singoli Stati la possibilità di dettare regole più precise e molto spesso lo strumento più utilizzato per l'ottenimento di prove elettroniche rimane la rogatoria (cfr. *supra* il § 1.5). Attualmente gli Stati membri hanno approcci diversi per quanto riguarda gli obblighi imposti ai prestatori di servizi, specialmente in relazione a procedimenti penali in cui sono coinvolti *providers* internazionali. Tale frammentazione crea incertezza per i soggetti coinvolti e può sottoporre i prestatori di servizi a obblighi e regimi sanzionatori differenti e talvolta in conflitto tra loro, 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.

Come noto, la prima norma convenzionale prescrive che gli Stati debbano fornire reciproca assistenza "in tempo reale", sia in materia di raccolta dei dati del traffico, sia in materia di intercettazione: rimangono in ogni caso ferme le condizioni e le procedure previste dai rispettivi diritti interni. La seconda norma, invece, dispone che le parti debbano fornire reciproca assistenza nella raccolta o registrazione in tempo reale di dati relativi a specifiche comunicazioni trasmesse attraverso l'uso di sistemi informatici, nella misura consentita dai trattati sottoscritti tra le stesse e dalle leggi interne.

---

affrontando i conflitti di legge e rendendo più rapido l'accesso alle prove elettroniche» (reperibile all'indirizzo https://eur-lex.europa.eu/resource.html?uri=cellar:b1826bff-2939-11e9-8d04-01aa75ed71a1.0018.02/DOC_1&format=PDF , visualizzato in data 23.6.2021).

[273] *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime* del 03 ottobre 2019, reperibile su
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf (visualizzato in data 23.6.2021).

[274] Cfr. F. Cajani, *Le richieste per finalità di giustizia rivolte agli Internet service providers esteri*, in AA.VV., *Cyber forensics e indagini digitali*, cit., p. 409.

[275] La Commissione europea, in occasione di una recente proposta di direttiva, ha previsto l'obbligo per i prestatori di servizi extra-europei di designare un rappresentante legale nell'Unione Europea incaricato di ricevere gli ordini di produzione e conservazione europei (cfr. EUROPEAN COMMISSION, *Proposal for a Directive of the European Parliament and of the Council - Laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, COM/2018/226 final - 2018/0107). L'obbligo di designare un rappresentante legale per tutti i fornitori di servizi che operano nell'Unione europea garantirebbe che gli ordini volti ad acquisire prove nei procedimenti penali abbiano sempre un destinatario chiaro. Ciò a sua volta renderebbe più semplice per i prestatori di servizi conformarsi a tali ordini, in quanto i rappresentanti legali sarebbero competenti per ricevere tali ordini, ottemperare agli stessi e farli eseguire per conto del prestatore di servizi. Peraltro, l'obbligo di designare un rappresentante legale per i prestatori di servizi non stabiliti nell'UE ma che offrono servizi nell'UE è già previsto da alcuni atti legislativi dell'UE applicabili in specifici settori, ad esempio nel già menzionato GDPR (articolo 27) e nella direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (articolo 18) (reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016L1148&from=EN, visualizzato in data 18.5.2021).

[276] Cfr. il § 1.5.

Entro tale scenario, si è soliti classificare i dati di interesse investigativo in tre macro categorie[277]:

I. *(basic) subscriber information*[278]: si tratta di dati che un utente fornisce al momento della registrazione (e-mail, numero di telefono, metodi di pagamento);

II. *traffic data*[279]: ossia i file di log concernenti le singole operazioni informatiche abbinate alle diverse tipologie di servizi;

III. *content data*[280]: trattasi dei dati attinenti al contenuto, per es. le fotografie, i video pubblicati etc.

Da gradi crescenti di "invasività" discende generalmente un diverso regime di cooperazione: normalmente, i SP esteri forniscono su base volontaria le prime due tipologie di dati. Quanto ai *content data*, di maggiore rilievo ai fini della presente ricerca, viene solitamente attivata una rogatoria, salvo sussistano situazioni di emergenza diversamente regolate a seconda degli Stati esteri in cui si trovano i *service providers*[281]. Su questo punto, occorre comunque considerare come il sistema di cooperazione internazionale in generale (e in particolare quello relativo ai rapporti di mutua cooperazione tra Italia e USA[282]) preveda la possibilità di ricorrere allo strumento della cd. *preservation data*, ovvero la richiesta di congelamento di dati collegati ad un *account*, tramite duplicazione del contenuto informativo dei dati dell'utente[283].

L'attuale assetto della Convenzione di Budapest non sembra fornire risposte adeguate a tutte le difficoltà che gli inquirenti si trovano ad affrontare nell'acquisizione di prove digitali. Per esempio, manca una regolamentazione specifica della cooperazione diretta con i *provider*, che è invece oggetto di una precisa disciplina nella proposta di regolamento e di direttiva da parte della Commissione

---

[277] Cfr. F. Cajani, *Le richieste per finalità di giustizia rivolte agli* Internet service providers *esteri*, cit., p. 414.

[278] Definiti dalla Convenzione di Budapest sulla criminalità informatica come «*the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a) the type of communication service used, the technical provisions taken thereto and the period of service; b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c)any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement*».

[279] « "*traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service*». Art. 1, lett. *d*), Convenzione di Budapest, cit.

[280] Nella Convenzione di Budapest non esiste una definizione di tale tipologia di dati. Tuttavia, il par. 209 dell'*Explanatory Report of the Budapest Convention* recita «*[content data] refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data*)».

[281] Peraltro, la maggior parte dei SP stranieri si sono da tempo attrezzati per rendere disponibili le *policies* al fine di facilitare il più possibile l'attività di polizia giudiziaria.

[282] Cfr. Il Trattato di mutua assistenza in materia penale tra il Governo della Repubblica Italiana e il Governo degli Stati Uniti d'America (Roma, 2006), reperibile all'indirizzo https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2009-03-27&atto.codiceRedazionale=009G0034 (visualizzato in data 13.5.2021).

[283] Cfr. F. Cajani, *Le richieste per finalità di giustizia rivolte agli Internet service providers esteri*, cit., p. 414.

europea (cfr. il § precedente). Peraltro, attraverso l'approvazione di un protocollo addizionale alla Convenzione di Budapest, che fissi regole più precise ed aggiornate sull'accesso transfrontaliero alle prove digitali, si sta cercando di trovare una soluzione al problema, permettendo inoltre di ottenere dati in maniera più veloce ed efficiente[284]. L'obiettivo principale consiste nel superamento della necessità di approcci nazionali individuali e non coordinati offrendo la certezza del diritto a livello internazionale.

2. "*Automatedly generated evidence*" e intelligenza artificiale: definizioni e ambiti applicativi

Come accennato *supra*, la trasformazione della società "digitale" sta determinando cambiamenti sostanziali non solo nel contesto in cui il crimine può verificarsi, ma anche nelle modalità con cui le indagini possono essere condotte[285]. Assicurare la giustizia costituisce un compito "umano" e il persistente impiego delle tecnologie digitali nella quotidianità degli individui sta ormai da tempo influenzando il modo in cui tali attività vengono svolte[286]. Peraltro, giova ricordare che il *digital turn* ha fornito non solo una moltitudine di dati suscettibili di essere utilizzati come prova nei procedimenti penali, ma anche nuovi metodi investigativi basati su *hacking*, *mining* e l'analisi di un'enorme quantità di dati (cfr. *supra* al § 1).

Entro tale contesto si colloca la diffusione applicativa dell'intelligenza artificiale (da qui in avanti IA) al fenomeno processuale penale[287], la cui «intrinseca imperscrutabilità dà luogo a non poche fibrillazioni rispetto alla congrua protezione dei diritti giudiziari riconosciuti, in genere, alle parti del

[284] Cfr. https://www.coe.int/en/web/cybercrime/t-cy-drafting-group e la bozza aggiornata e pubblicata in data 17.11.2021, reperibile all'indirizzo https://rm.coe.int/0900001680a2aa1c. Sul punto cfr. K.Pivcevic, *Privacy concerns linger around new EU data sharing Protocol*, reperibile all'indirizzo https://www.biometricupdate.com/202109/privacy-concerns-linger-around-new-eu-data-sharing-protocol (visualizzato in data 28.2.2022).

[285] Cfr. P. Comoglio, *Prefazione*, in J. Nieva-Fenoll, *Intelligenza artificiale e processo*, Giappichelli, Torino, 2019, p. 12.

[286] Cfr. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, 2020, p. 5.

[287] Sull'argomento cfr. *ex multis* il lavoro pioneristico di L. Luparia, *Prova giudiziaria e ragionamento artificiale: alcune possibili chiavi di lettura*, in AA.VV., *Il concetto di prova alla luce dell'intelligenza artificiale*, (a cura di) J. Sallantin e J.J. Szczeciniarz, Giuffreè, Milano, 2005, pp. 14 e ss., M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra stati uniti ed Europa*, in *www.dirittopenalecontemporaneo.it*, 29 maggio 2019, p. 1, G. Canzio, *Intelligenza artificiale e processo penale*, in *Cass. pen.*, fasc.3, 1.3.2021, p. 797, M. Caianiello, *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 29, (2021), pp. 1-23, J. Nieva-Fenoll, *Intelligenza artificiale e processo*, (trad. a cura di) P. Comoglio, Giappichelli, Torino, 2019, pp. 7 e ss., M. Taruffo, *Judicial decision and Artificial Intelligence*, in *Artificial Intelligence and Law*, 1998, pp. 311 e ss. Si concorda con A. Garapon, J. Lassègue, *La giustizia digitale. Determinismo tecnologico e libertà*, Il Mulino, Bologna, 2021, p. 143, i quali affermano che «la nostra epoca è affascinata dall'intelligenza artificiale, che, ad esempio, annuncia di poter ricostruire il viso di un individuo a partire da una goccia di sangue. Se tale scoperta fosse confermata, si aggiungerebbe all'efficacia probatoria del Dna, che consente di identificare un individuo a partire da un capello».

processo, in particolare all'imputato, dalla Costituzione e dalle Carte sovranazionali dei diritti umani»[288] (cfr. *infra* il capitolo III, §§ 2 e ss.).

Per vero - anche in questo ambito[289] - non è possibile fare riferimento ad un'unica e condivisa definizione di intelligenza artificiale[290]. Parte della dottrina la descrive come «la tecnologia che permette ad un computer di analizzare grandi quantità di dati e, sulla base della conoscenza e dell'esperienza acquisita, adottare comportamenti intelligenti o proporre decisioni»[291]. La

---

[288] Cfr. G. Ranaldi, *Processo penale e prova informatica: profili introduttivi*, in *Diritto Pubblico Europeo online* n. 2/2020, p. 18. La riflessione dell'Autore si giustifica col fatto che l'IA è una disciplina connotata da un forte tratto di interdisciplinarietà: la materia ricomprende *ex multis* l'ingegneria, la matematica, il diritto, la filosofia, l'etica, la sociologia e la psicologia.

[289] Diverse difficoltà di definire determinati ambiti sono già emerse in precedenza, cfr. il capitolo I, § 1 e il capitolo II, § 1.

[290] Cfr. S. Quattrocolo, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, p. 123, M. Ebers, *Regulating AI and Robotics: Ethical and Legal Challenges*, in AA.VV., *Algorithms and Law*, (a cura di) M. Ebers, S. N. Navarro, Cambridge, Cambridge, University Press, 2019, pp. 6 e ss. Sul punto, A. Krausová, *Intersections between Law and Artificial Intelligence*, in *International Journal of Computer* (IJC) (2017) Volume 27, No 1, pp. 57-58 afferma che «*there exists a number of definitions of AI but none of them is universally pertinent while being truly unequivocal at the same time*». Cfr. anche F. Donati, *Intelligenza artificiale e giustizia*, in *Rivista AIC*, 1/2020, 2.3.2020, p. 415, M. Ienca, *Intelligenza². Per un'unione di intelligenza naturale e artificiale*, Rosenberg & Sellier, Torino, 2019, p. 13 e J. Nieva-Fenoll, *Intelligenza artificiale e processo*, cit., p. 8. Peraltro, la proposta di regolamento del 21.4.2021 "*on a European approach for Artificial Intelligence*" (cfr. *infra*, il § 2.2.1) ha introdotto un'unica definizione adattabile in vista di sviluppi futuri. In particolare, l'art. 3 stabilisce che: «'*artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*». Cfr. COM(2021) 206 final. La definizione proposta non è andata esente da critiche, sul punto cfr. M. Ebers, V.R.S. Hoch, F. Rosenkranz, H. Ruschemeier, B. Steinrötter, *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society*, in *(RAILS). J.* 2021, 4(4), pp. 589-603. Il Consiglio dell'Unione europea ha di recente diffuso un primo testo di modifica delle disposizioni contenute nella proposta di regolamento della Commissione europea (COUNCIL OF THE EUROPEAN UNION, *Presidency compromise text*, 2021/0106(COD), 29.11.2021, proponendo di modificare la definizione come segue: «'*artificial intelligence system' (AI system) means a system that (i) receives machine and/or human-based data and inputs, (ii) infers how to achieve a given set of human-defined objectives using learning, reasoning or modelling implemented with the techniques and approaches listed in Annex I, and (iii) generates outputs in the form of content (generative AI systems), predictions, recommendations or decisions, which influence the environments it interacts with*» (Art. 3, par. 1). Il Parlamento europeo, dal canto suo, tramite il COMMITTEE ON LEGAL AFFAIRS FOR THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION AND THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft Opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts* (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 2.3.2022, p. 24, ha proposto di definire un sistema di intelligenza artificiale come «*a machine based system that is developed with the techniques and approaches listed in Annex I and is capable of influencing the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives. It uses machine and/or human-based data and inputs to (i) perceive real and/or virtual environments; (ii) abstract these perceptions into models through analysis in an automated manner (e.g., with machine learning), or manually; and (iii) use model inference to formulate options for outcomes. AI systems are designed to operate with varying levels of autonomy*» (Articolo 3, par. 1). Quasi contestualmente, sempre il Parlamento europeo, tramite il COMMITTEE ON INDUSTRY, RESEARCH AND ENERGY FOR THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION AND THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS *on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) ha proposto l'ulteriore definizione: «*'artificial intelligence system' (AI system) means a machine-based system that can for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments; AI systems can be designed to operate with varying levels of autonomy and can be developed with one or more of the techniques and approaches listed in Annex I*» (Art. 3, par. 1).

[291] Cfr. F. Donati, *Intelligenza artificiale e giustizia*, cit., p. 415. Per un'approfondita ricostruzione della definizione di IA cfr. G. Romano, *Diritto, robotica e teoria dei giochi: riflessioni su una sinergia*, in AA.VV., *Diritto e intelligenza artificiale*, (a cura di) G. Alpa, Pacini eds., Pisa, 2020, p. 105, S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, cit., pp. 7-8. Sul punto giova ricordare la *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions*- Artificial Intelligence for Europe, il cui testo ufficiale è reperibile su https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-

Commissione europea, tentando di fornire una definizione leggermente più ampia, la colloca in «quei sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere in software che agiscono nel mondo virtuale (per esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale); oppure dispositivi hardware che incorporano l'IA (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose)»[292]. L'IA costituirebbe in questo senso «quel settore dell'informatica con oggetto la teoria, le tecniche e le metodologie che permettono di progettare sistemi hardware e software in grado di elaborare delle prestazioni "assimilabili" all'intelligenza umana»[293]. Da ciò si evince che i progressi compiuti nell'ambito del calcolo e la crescente disponibilità di dati sono fattori del tutto determinanti per l'attuale sviluppo di IA: come si vedrà meglio *infra*, è fondamentale che tali dati siano il più possibile neutri, spogliati di elementi che possano condurre a pregiudizi o discriminazioni legate alla razza, al sesso, alle opinioni politiche etc.[294].

In altre parole, alcuni strumenti di IA sono in grado di «fornire prestazioni assimilabili a quelle dell'intelligenza umana e, cioè, l'abilità di risolvere problemi o svolgere compiti e attività tipiche della mente e del comportamento umano»; ne consegue una tendenza di tale specifica tecnologia a comportarsi "come un essere umano"[295], ossia, nei sistemi più avanzati, «la capacità non soltanto di trattazione automatizzata di enormi quantità di dati e di fornire le risposte per le quali sono stati programmati, ma anche di acquisire, sulla base di appositi algoritmi di apprendimento, l'attitudine a formulare previsioni o assumere decisioni»[296].

Pertanto, aldilà dello sforzo esegetico di individuare una definizione universale ed esaustiva, il tratto tipico dei sistemi di intelligenza artificiale sembra proprio quello di un'attitudine a simulare e

237-F1-EN-MAIN-PART-1.PDF (visualizzato in data 19.4.2021), ove l'IA viene definita come «*Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications*)».

[292] V. nota precedente. Cfr. anche A. Krausová, *Intersections between Law and Artificial Intelligence*, cit., p. 58 richiama la definizione secondo la quale «*an AI system includes both hardware and software components. It thus may refer to a robot, a program running on a single computer, a program run on networked computers, or any other set of components that hosts an AI*».

[293] Cfr. C. Parodi, V. Sellaroli, *Sistema penale e intelligenza artificiale: molte esperienze e qualche equivoco*, in *www.dirittopenalecontemporaneo.it*, p. 64. A tal proposito, v. anche la definizione del matematico statunitense Marvin Minsky che la definisce come «*the science of making machines do things that would require intelligence if done by man*», richiamata da S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, cit., p. 102.

[294] Cfr. C. Cavaceppi, *L'intelligenza artificiale applicata al diritto penale*, in AA.VV., *Intelligenza artificiale. Algoritmi giuridici* Ius condendum *o "fantadiritto"?*, (a cura di) G. Taddei Elmi, A. Contaldo, Pacini editore, Pisa, 2020, p. 99.

[295] Cfr. D. Polidoro, *Tecnologie informatiche e procedimento penale: la giustizia penale messa alla prova dall'intelligenza artificiale*, in *Arch. Pen*., Fasc. n. 3, 2020 (Web), p. 4 e J. Nieva-Fenoll, *Intelligenza artificiale e processo*, cit., p. 8.

[296] Cfr. A. Traversi, *Intelligenza artificiale applicata alla giustizia: ci sarà un giudice robot?*, in *www.questionegiustizia.it.*

replicare i meccanismi intellettivi di un essere umano[297]. A tal proposito, un elemento chiave è costituito dal concetto base di algoritmo[298], ossia un'istruzione matematica (o codice) impiegata al fine di risolvere un problema, dare una risposta ad un quesito ovvero svolgere determinate funzioni[299].

I delineati riferimenti concettuali consentono di intuire gli ambiti di interazione tra la giustizia penale e, per l'appunto, i sistemi di intelligenza artificiale. A tal proposito, sebbene la materia esuli da questo studio, l'implementazione dei *tools* di IA ha cominciato a profilarsi in materia giudiziaria con particolari sviluppi nell'ambito della cd. "giustizia predittiva", ossia introducendo la possibilità di formulare previsioni sia sull'esito di una determinata controversia tramite correlazioni tra enormi quantità di dati tratti da precedenti decisioni giudiziarie adottate in casi analoghi, sia al momento della commisurazione della pena, rispetto ad un'eventuale prognosi di recidiva sulla base di algoritmi di *risk assessment*[300]. Trattasi di strumenti «*that use socioeconomic status, family background,*

---

[297] Giova comunque ricordare quanto affermato da F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. uomo*, 2019, 10, 2 secondo cui occorre «sgombrare il campo da un paio di equivoci: - innanzitutto, quando parliamo di IA non dobbiamo necessariamente pensare ad un umanoide simile in tutto e per tutto all'essere umano: l'umanoide può essere, sì, un'applicazione di IA (forse la più eclatante), ma di certo non l'unica e non, almeno nella fase attuale, la più rilevante dal punto di vista pratico; – in secondo luogo, per quanto possa essere suggestivo parlare di intelligenza artificiale, occorre rimarcare che, in realtà, "poco, oltre alla speculazione e a un modo di pensare ingenuo, collega il lavoro odierno nel campo dell'IA ai misteriosi meccanismi della mente umana; in realtà, almeno a questo stadio, si tratta di una disciplina ingegneristica con relazioni più che altro metaforiche e di 'ispirazione' con gli organismi biologici", tanto più che l'intelligenza (quella degli esseri umani, prima ancora che quella delle macchine), per quanto sia oggetto di numerosissimi studi di psicologi, biologi e neuroscienziati, costituisce ancora un concetto indeterminato».

[298] In T. Gillespie, *The relevance of Algorithms*, in AA.VV., *Media Technologies*, (a cura di) T. Gillespie, P. Boczkowki, K. Foot, Cambridge US, 2014, p. 167, «*algorithms need not be software: in the broadest sense, they are encoded procedures for transforming input data into a desired output, based on specified calculations. The procedures name both a problem and the steps by which it should be solved*». In J. Nieva-Fenoll, *Intelligenza artificiale e processo*, cit., p. 9 l'"algoritmo" viene definito come «lo schema esecutivo della macchina che memorizza tutte le operazioni decisionali in base ai dati che progressivamente elabora». Sul punto v. anche G. M. Schneider, J. L. Gersting, *Informatica*, Santarcangelo di Romagna, Maggioli Editore, 2013. In altre parole, esso costituisce «*a series of steps undertaken in order to solve a particular problem or accomplish a defined outcome*». R. Kitchin, Thinking critically about and researching algorithms, (2017) 20(1) *Information, Communication and Society*, pp. 1-14. La stessa definizione è presente sia in S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, cit., p. 8 sia in M. Ebers, *Regulating AI and Robotics: Ethical and Legal Challenges*, in AA.VV., *Algorithms and Law*, (a cura di) M. Ebers, S. N. Navarro, Cambridge, Cambridge, University Press, 2019, p. 6. Giova ricordare altresì una recente pronuncia del Consiglio di Stato (n. 7891 del 25.11.2021) ove il Collegio ha riconosciuto la nozione comune e generale di "algoritmo", quale «*sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato*». Da tenere distinto è il campo dell'intelligenza artificiale, ove l'algoritmo, essendo ivi applicate tecniche di *machine learning* (o apprendimento automatico) ovvero di *deep learning* (apprendimento profondo), non si limita ad eseguire solamente le attività preimpostate (come fa l'algoritmo di base tradizionale) ma, al contrario, elabora sistematicamente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un procedimento di apprendimento automatico. Per un commento della sentenza v. G. Tavella, *Consiglio di Stato: la perimetrazione tecnica della nozione di "algoritmo di trattamento"*, 13.1.2022, in *Fondazione Leonardo – Civiltà delle macchine*, reperibile all'indirizzo https://www.civiltadellemacchine.it/it/rivista-trimestrale (visualizzato in data 24.1.2022).

[299] Cfr. F. Donati, *Intelligenza artificiale e giustizia*, cit., p. 416.

[300] A tal proposito, si vedano alcune esperienze italiane tra cui il *Key crime*, adottato dalla Questura di Milano che ha portato a risultati assai significativi (C. Morabito, *La chiave del crimine*, consultabile all'indirizzo https://www.poliziadistato.it/statics/16/la-chiave-del-crimine.pdf, visualizzato in data 30.6.2021; M. Serra, Rapinatore seriale catturato grazie al software "*Key crime*", consultabile all'indirizzo https://www.lastampa.it/milano/2018/01/05/news/rapinatore-seriale-catturato-grazie-al-software-key-crime-1.33963498, visualizzato in data 30.6.2021), oppure al *X-Law*, un software elaborato dalla Questura di Napoli e completato dal Dipartimento di Pubblica Sicurezza del Ministero dell'Interno e usato in

neighbourhood crime, employment status, and other factors to reach a supposed prediction of an individual's criminal risk, either on a scale from "low" to "high" or with specific percentages»[301].

L'altra area nella quale si sta sempre di più consolidando l'uso della tecnologia di IA e che risulta di particolare interesse per la presente ricerca, è quella investigativo-probatoria, delle cd. "*automatedly generated evidence*"[302]; nella fase delle indagini, infatti, si fa un uso sempre più ampio di sistemi basati su prove algoritmiche in senso lato[303]. In questo ambito, l'attività di indagine fondata su sistemi di IA si intreccia con quella della prova digitale (cfr. *supra*, il § 1). A tal proposito, si è soliti distinguere fra

---

diverse realtà del nostro Paese (cfr. https://corrieredelveneto.corriere.it/venezia-mestre/cronaca/18_novembre_16/venezia-l-algoritmo-che-prevede-furti-avvisa-polizia-colpo-sventato-d62fe1fc-e9ab-11e8-9475-b8ef849c8bde_preview.shtml?reason=unauthenticated&cat=1&cid=_I9mvdW3&pids=FR&cr, visualizzato in data 30.6.2021). In letteratura, senza alcuna pretesa di esaustività, cfr. F. Falato, *L'inferenza generata dai sistemi esperti e dalle reti neurali nella logica giudiziale*, in *Arch. Pen*., 2020, p. 2, F. Maggino, G. Cicerchia, *Algoritmi, etica e diritto*, in *Diritto dell'Informazione e dell'Informatica* (Il), fasc.6, 1.12.2019, p. 1161, M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *www.penalecontemporaneo.it*, F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. uomo* (web), 2019, C. Castelli, D. Piana, *Giustizia predittiva. La qualità della giustizia in due tempi*, in *Quest. Giust.* (web), 2019, D. Dalfino, *Stupidità (non solo) artificiale, predittività e processo*, in *Quest. Giust*. (web), 2019, E. Fronza, C. Caruso, *Ti faresti giudicare da un algoritmo?, Intervista A. Garapon*, in *Quest. giust*. (web), 2018, 4, p. 196, S. Quattrocolo, *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Rev. Italo-espanola derecho procesal*, 2018, 2, p. 12, G. Riccio, *Ragionando su intelligenza artificiale e processo penale*, in *Arch. Pen*., 2019, 3, U. Pagallo, S. Quattrocolo, *The impact of AI in criminal law and its two fold procedures*, in AA.VV. *Research Handbook on the law of artificial intelligence*, (a cura di) W. Barfield, U. Pagallo, Edward Elgar Publishing, Cheltenam, 2018, pp. 318 e ss., G. Vossos, J. Yeleynikow, D. Hunter, *Design Intelligence Litigation Support Tools: The IKBALS Perspective*, in *2 Law, Computers &Artificial Intelligence*, 1993, pp. 77 e ss., S. Smyth, *Biometrics, surveillance and the law. Societies of restricted access, discipline and control*, Routledge, New York, pp. 15 e 76; M. Catanzariti, *Enhancing Policing through Algorithmic Surveillance*, in AA.VV. *The Fight Against Impunity in EU Law*, (a cura di) L. Marin, S. Montaldo, Hart Publishing, New York, 2020, pp. 239 e ss., M. M. Plesnicar, A. Završnik, P. Šarf, *Fighiting Impunity with New Tools: How Big Data, Algorithms, Machine Learning and AI Shape the New Era of Criminal Justice*, in AA.VV., *The Fight Against Impunity in EU Law*, cit., p. 259. Il dibattito dottrinale non si incentra esclusivamente su chi è favorevole o no all'adozione di questi sistemi, ma su aspetti specifici concernenti il tema della responsabilità, del trattamento dei dati personali, della standardizzazione delle decisioni, della parità di trattamento e del rispetto dei diritti fondamentali. Si tratta di punti di discussione complessi, che assumono dei risvolti non soltanto giuridici, ma anche etici, tanto da condurre recentemente alla introduzione della Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi (adottata dalla CEPEJ nel corso della sua 31ª Riunione plenaria (Strasburgo, 3-4 dicembre 2018).

[301] In tal senso, ELECTRONIC PRIVACY INFORMATION CENTER, *Algorithms in the Criminal Justice System*, reperibile all'indirizzo https://epic.org/ai/criminal-justice/index.html (visualizzato in data 30.6.2021).

[302] L'espressione, come già anticipato *supra*, è di S. Quattrocolo, *Equità del processo penale e* automated evidence *alla luce della Convenzione europea dei diritti dell'uomo*, in *Revista Italo-Española de Derecho Procesal*, 2019, pp. 2 e ss. Cfr. anche C. Cesari, *L'impatto delle nuove tecnologie sulla giustizia penale- un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1169, F. Palmiotto, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in AA.VV., *Algorithmic Governance and Governance of Algorithms, Legal and Ethical Challenges*, (a cura di) M. Ebers, M. Cantero Gamito, Springer, Berlin, 2020, p. 52, G. Ranaldi, *Processo penale e prova informatica*, cit., p. 19; M. Daniele, *La prova digitale nel processo penale*, in *Riv. Dir. Proc.*, 2011, p. 288, M. Pittirutti, *Digital evidence e procedimento penale*, Giappichelli, Torino, 2017, AA.VV., *Il concetto di prova alla luce dell'intelligenza artificiale*, (a cura di) J. Sallantin, J.J. Szczeciniarz, Giuffrè, Milano, 2005 e, con riferimento al rapporto tra *artificial intelligence* e prova penale, si veda L. Luparia, *Prova giudiziaria e ragionamento artificiale: alcune possibili chiavi di lettura*, in AA.VV., *Il concetto di prova alla luce dell'intelligenza artificiale*, cit., p. 14, J. Nieva-Fenoll, *Intelligenza artificiale e processo*, cit., p. 14, Sara Smyth, S. Smyth, *Biometrics, surveillance and the law. Societies of restricted access, discipline and control*, Routledge, New York, p. 71.

[303] L'impiego di tali sistemi è destinato a crescere con la diffusione dell'*Internet of things*, v. sul punto U. Pagallo, S. Quattrocolo, *The impact of AI on criminal law, and its twofold procedures*, in AA.VV., *Research Hanbook on the Law of Artificial Intelligence*, (a cura di) W. Barfield, U. Pagallo, Edward Elgar publishing, Cheltenham-Northampton, 2018, p. 385.

intelligenza artificiale "forte" (*strong AI*), con cui s'intende la creazione delle cd. "*machine learning*"[304], ossia meccanismi di auto-apprendimento in grado di "imparare" il mondo esterno[305], e una "debole" (*weak AI*), coincidente con quella che estrae sistemi complessi di valutazione sulla base di grandi volumi di dati immessi dall'uomo[306]. Lo scopo che accomuna entrambe le forme di intelligenza artificiale è quello di fornire prestazioni assimilabili a quelle dell'intelligenza umana[307]. La maggior parte di questi sistemi, invero, è progettata sul modello delle reti neuronali del cervello umano[308], il che è reso possibile dalla correlazione e interpretazione dei cd. "*big data*"[309], utilizzati per esempio per riconoscere una voce o un volto.

È chiaro che il procedimento di identificazione o autenticazione di un individuo risulti oltremodo agevolato dall'impiego di tecniche di intelligenza artificiale: queste ultime consentono di estrarre caratteristiche fisionomiche non direttamente visibili, rendendo più agevoli i confronti e le valutazioni metriche. In tal senso, il vantaggio per il lavoro degli investigatori sul piano sia della velocità sia dell'efficienza è davvero sorprendente[310].

Tuttavia, molto più di quanto sia possibile osservare sul territorio nazionale, a livello mondiale l'applicazione di tecniche di intelligenza artificiale al riconoscimento automatico costituisce – oggi più che mai – un tema estremamente dibattuto[311]. Più nel dettaglio, prestigiose istituzioni scientifiche e associazioni per la tutela di diritti e libertà civili hanno segnalato, in diverse circostanze, i rischi connessi ad un utilizzo sregolato di certe forme di intelligenza artificiale, sia per un'elevata probabilità di sviluppo di risultati non attendibili, sia per la strumentalizzazione a fini discriminatori e di controllo

---

[304] L'espressione "*machine learning*" si riferisce a sistemi che riescono ad estrarre automaticamente modelli significativi da grandi quantità di dati. Cfr. al riguardo S. Shalev Shwartz, S. Ben David, *Understanding Ma-chine Learning: From Theory to Algorithms*, Cambridge University Press, New York, 2014.

[305] Cfr. M. Ebers, *Regulating AI and Robotics: Ethical and Legal Challenges*, in AA.VV., *Algorithms and Law*, (a cura di) M. Ebers, S. N. Navarro, Cambridge, Cambridge, University Press, 2019, p. 7.

[306] Cfr. R. Lopez, *Riconoscimento facciale tramite software e individuazione del sospettato*, in AA.VV., *Pre-Investigazioni*, (a cura di) A. Scalfati, Giappichelli, Torino, 2020, p. 296 e F. Maggino, G. Cicerchia, *Algoritmi, etica e diritto*, cit., p. 1161 e T. Taulli, *Artificial Intelligence Basics*, Apress, Berkeley, 2019, p. 4.

[307] I sistemi più avanzati sono in grado di elaborare previsioni o di effettuare valutazioni grazie ad appositi algoritmi di apprendimento che trattano in via automatizzata un'enorme quantità di dati.

[308] Per un approfondimento sulle diverse tecniche di IA applicate ai dati biometrici cfr. B. S. Maaya, T. Asha, *Current Trends of Machine Learning Techniques in Biometrics and its Applications*, in AA.VV., *AI and Deep Learning in Biometric Security*, (a cura di) G. Jaswal, V. Kanhangad, R. Ramachandra, CRC Press, Boca Raton, 2021 e G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., pp. 55 e ss.

[309] Per una definizione cfr. T. Taulli, *Artificial Intelligence Basics*, cit., pp. 23 e ss. e G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 78.

[310] Con riferimento al vantaggio in termini di calcolo nell'utilizzo di sistemi di intelligenza artificiale cfr. D. Ben-Ari, Y. Frish, A. Lazovski, U. Eldan, D. Greenbaum, *Artificial Intelligence in the Practice of Law: An Analysis and Proof of Concept Experiment*, in *23 Richmond Journal of Law & Technology*, 2017, p. 21. Riguardo alle tecniche di intelligenza artificiale applicate al riconoscimento facciale, sia consentito il riferimento a E. Sacchetto, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *www.lalegislazionepenale.it*, 16.10.2020.

[311] Sul punto cfr. R. Lopez, *Riconoscimento facciale tramite software e individuazione del sospettato*, in AA.VV., *Pre-investigazioni*, Giappichelli, Torino, 2020, pp. 301 e ss.

politico e sociale, cui il suo impiego si presta[312]. Il rischio di errori o di discriminazioni non può essere in alcun modo sottovalutato. I sistemi di intelligenza artificiale possono restituire risultati fuorvianti per due generi di fattori: *in primis*, il funzionamento del sistema può presentare problemi di "apprendimento", derivanti da un impiego non corretto dei dati considerati nella fase preliminare in cui il software elabora i propri modelli decisori (cd. "*training data*"). In particolare, qualora questi dati non fossero stati raccolti correttamente, ovvero contenessero errori, l'attendibilità dei risultati ne risulterebbe inevitabilmente compromessa[313]. Un secondo fattore è proprio la cd. "discriminazione statistica", ossia l'esistenza di condizionamenti causati da rilevazioni statistiche effettuate precedentemente. Addirittura si ritiene che tale tipologia di discriminazione sia già presente quando non vengono impiegate tecniche di intelligenza artificiale, dal momento che chi valuta e prende una determinata decisione spesso, in assenza di dati e informazioni su un determinato aspetto, tende a sostituire l'informazione mancante con altre disponibili[314]. Peraltro, il rischio di discriminazioni di questo genere risulta ancora maggiore quando sono impiegati sistemi di IA[315]. A tal proposito, come si approfondirà meglio *infra*, uno dei principi etici fondamentali da tenere in considerazione in tutte le fasi di progettazione, sviluppo e applicazione di uno strumento di IA è proprio quello di non discriminazione (cfr. il § 2.2). Prima di addentrarci in un'analisi, seppur per brevi cenni, del catalogo dei requisiti che un sistema di IA è chiamato a rispettare per potersi definire "etico", alla luce del recente sviluppo normativo europeo, giova fornire al lettore una ricostruzione degli strumenti giuridici introdotti negli ultimi anni che hanno portato all'attuale quadro normativo.

2.1 Il quadro normativo di riferimento: una ricostruzione dello stato dell'arte

Se a livello nazionale non è ancora stato introdotto alcuno strumento normativo specifico che regoli - espressamente e organicamente - l'applicazione della tecnologia di IA in ambito giudiziario[316], in Europa e, più in generale, a livello sovranazionale si registra invece - ormai da qualche tempo - una

[312] Cfr. R. Lopez, *Riconoscimento facciale tramite software*, cit., p. 302.
[313] Cfr. F. Donati, *Intelligenza artificiale e giustizia*, cit., p. 422.
[314] Cfr. F. Donati, *Intelligenza artificiale e giustizia*, cit., p. 423.
[315] Si ricorda un approdo giurisprudenziale del tutto all'avanguardia da parte del Cons. Stato, sez. VI, 13.12.2019, n. 8472 in cui si sottolinea l'importanza per il titolare del trattamento di dati di mettere in atto tecniche organizzative adeguate, al fine di garantire che siano rettificati i fattori che comportano inesattezze dei dati e sia così minimizzato il rischio di errori, al fine di garantire la sicurezza dei dati personali, secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche.
[316] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, p. 120. Non mancano, tuttavia, disposizioni normative di diritto primario, cogenti, che regolamentano alcuni aspetti di particolare importanza dell'avvento dell'IA in ambito giudiziario. Trattasi di disposizioni normative che comunque provengono da istanze sovranazionali, tra cui si ricorda, come sarà meglio approfondito *infra*, il regolamento (UE) 2016/679 (GDPR) direttamente applicabile all'interno degli Stati membri, la cui disciplina sulle decisioni automatizzate va completata con la già citata direttiva 680/2016/UE, adottata il 27.4.2016, recepita con il d.lgs. n. 51/2018.

diffusa consapevolezza circa l'utilità dell'impiego di tali tecniche a servizio della giustizia[317]. In particolare, il dibattito odierno ha ad oggetto non tanto la possibilità di impiegare tali sistemi di IA in questo ambito, quanto il necessario rispetto dei diritti e dei valori fondamentali potenzialmente condizionati dall'impiego di queste tecniche. O meglio, l'effettiva *querelle*, opportunamente avviata a livello europeo[318], concerne le modalità con cui i sistemi giudiziari si organizzeranno, nel prossimo futuro, per far fronte all'implementazione sistematica di tali strumenti tecnologici, senza divenirne "vittime"[319] e la creazione di un quadro giuridico efficace per il loro utilizzo al fine di assicurare il rispetto dei diritti e dei valori fondamentali dell'Unione europea. A tal proposito, un primo esito del fenomeno è rappresentato dal già citato regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio (da qui in avanti GDPR inteso come *General data protection regulation*) del 27 aprile 2016, avente ad oggetto la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, che abroga la direttiva 95/46/CE (cfr. il capitolo I, § 1). Il dato normativo, per i profili che interessano la presente ricerca, è completato dalle linee guida *Working Party* 251 del 3 ottobre 2017 sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione, elaborate dal Comitato europeo per la protezione dei dati personali[320].

Posto che nel regolamento non si trova alcun riferimento espresso sull'uso dell'intelligenza artificiale nei procedimenti giudiziari, vi sono ulteriori indicazioni generali[321] che possono essere prese in considerazione anche per la materia in oggetto[322]. La correttezza del processo decisionale informatico, infatti, deve essere garantita in tutti i settori nei quali vengono effettuate scelte che possano incidere sui diritti delle persone[323]. Più nel dettaglio, intuitivamente i principi generali valevoli per ogni forma di trattamento di dati personali si applicano anche ai sistemi di IA (art. 5 GDPR). Come noto, l'art. 15 (lett. *h*) stabilisce che l'interessato ha il diritto di conoscere l'esistenza di un processo decisionale automatizzato e, in tal caso, di ricevere «informazioni significative sulla

[317] Cfr. M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra stati uniti ed Europa*, cit., p. 12 e M. Caianiello, *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 29, (2021), p. 1.

[318] Tra i compiti conferiti all'allora Comunità economica europea (CEE) particolare rilievo aveva assunto quello previsto dall'art. 2 del relativo Trattato istitutivo e cioè il compito di promuovere «un'espansione continua ed equilibrata, una stabilità accresciuta, un miglioramento sempre più rapido del tenore di vita e più strette relazioni fra gli Stati che ad essa partecipano». Art. 2, Trattato istitutivo della Comunità economica europea (CEE), firmato a Roma il 25 marzo 1957 ed entrato in vigore il 1° gennaio 1958.

[319] Cfr. M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., p. 12.

[320] WP 251 – *Linee Guida su profilazione e processi decisionali automatizzati*, reperibile su https://ec.europa.eu/newsroom/document.cfm?doc_id=47742 (visualizzato il 4.5.2021).

[321] "Ulteriori" poiché nel capitolo I si è già fatto cenno al regolamento (UE) 2016/679 per la definizione di "dato biometrico" (cfr. il § 1).

[322] Infatti, al fine di assicurare la trasparenza e la correttezza delle decisioni assunte attraverso l'impiego di sistemi di IA possono essere invocate le disposizioni del GDPR. Cfr. F. Donati, *Intelligenza artificiale e giustizia*, cit., p. 424.

[323] Cfr. F. Donati, *Intelligenza artificiale e giustizia*, cit., p. 425.

logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato»[324]. E ancora, gli articoli 35 e ss. del GDPR disciplinano uno specifico procedimento di valutazione d'impatto sulla protezione dei dati, ogni volta in cui un determinato tipo di trattamento, specie se prevede l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone.

La norma più conferente in questo ambito è fuor di dubbio l'art. 22, che permette all'interessato di opporsi a decisioni che producano effetti significativi nella sua sfera giuridica e che siano basate "unicamente" su un trattamento automatizzato, ossia di decisioni nelle quali non vi è alcun coinvolgimento umano nel processo decisionale[325]. In questo modo, il legislatore europeo ha fissato alcune condizioni di base al cui ricorrere è consentita la decisione interamente automatizzata, aprendo di fatto la via a nuove forme di giustizia dai contorni ancora da definire[326]. La "decisione automatizzata" costituisce una nozione assai ampia, comprensiva non solo di provvedimenti giurisdizionali, ma anche di valutazioni delle prove, basate su elaborazioni algoritmiche di dati e produttive di effetti giuridici[327], le quali non prevedono l'intervento umano né in fase istruttoria, né in fase di valutazione, sebbene la decisione sia da imputarsi formalmente all'uomo.

Le linee guida WP 251 del 3 ottobre 2017 risultano piuttosto rigorose sul punto prevedendo possibili aggiramenti del divieto di interventi umani meramente simbolici e non sostanziali: ne consegue un procedimento nel quale l'intervento umano, seppur presente al momento decisionale, è in realtà puramente formale, rientrando l'ipotesi nel divieto posto dalla norma[328].

Per vero, sono state previste diverse eccezioni, relative alle ipotesi in cui il trattamento automatizzato dei dati sia necessario per la conclusione o l'esecuzione di un contratto, o sia autorizzato dal diritto dell'Unione o di uno Stato membro o ancora si basi sul consenso esplicito dell'interessato. Rimane ferma, al comma 3, la previsione che impone al titolare del trattamento l'obbligo di adottare le misure appropriate per tutelare i diritti, le libertà e gli interessi legittimi del soggetto interessato. Tra queste misure minime di tutela la norma prevede il diritto di ottenere l'intervento umano del

---

[324] Sul punto cfr. F. Pizzetti, *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in AA.VV., *Intelligenza artificiale, protezione dei dati personali e regolazione*, (a cura di) F. Pizzetti, Giappichelli, Torino, 2018, p. 30.

[325] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., p. 196 e B. Galgani, *Habeas data e garanzie fondamentali*, in *Arch. pen.*, 2019, p. 20.

[326] Si esclude da questo ambito il trattamento dei dati a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali (art. 2 c. 1 lett. *d*). M. Catanzariti, *Enhancing Policing through Algorithmic Surveillance*, in AA.VV. *The Fight Against Impunity in EU Law*, (a cura di) L. Marin, S. Montaldo, Hart Publishing, New York, 2020, pp. 249 e ss.

[327] L'art. 4, n. 4 del regolamento stabilisce che nella nozione sia compresa «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

[328] Cfr. C. Cavaceppi, *L'intelligenza artificiale applicata al diritto penale*, in AA.VV., *Intelligenza artificiale. Algoritmi giuridici Ius condendum o "fantadiritto"?*, (a cura di) G. Taddei Elmi, A. Contaldo, Pacini editore, Pisa, 2020, p. 128.

titolare del trattamento, di esprimere la propria opinione e di contestarne la decisione. Ne consegue che tali disposizioni potranno essere invocate da chi nutra un interesse a verificare la correttezza del procedimento seguito dal sistema di IA.

L'articolo 22 par. 4, poi, vieta il processo decisionale automatizzato che utilizzi dati personali sensibili di cui all'art. 9 par. 1, salvo il caso in cui il soggetto interessato abbia manifestato il proprio consenso[329], ovvero il trattamento sia necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione europea o degli Stati membri, nonché proporzionato alla finalità perseguita, rispetti il diritto alla protezione dei dati e preveda misure idonee per tutelare i diritti fondamentali dell'interessato. Tra questi diritti non figura quello all'informazione sul funzionamento del procedimento decisionale ed in particolare sull'algoritmo utilizzato[330]. Trattasi di una lacuna piuttosto vistosa, in quanto il mancato riconoscimento del diritto di accedere ai processi decisionali automatizzati che presiedono l'adozione della decisione rischia di trasformare l'effettività del sistema dei diritti configurati nel regolamento in un quadro giuridico del tutto apparente[331]. Come si approfondirà meglio *infra*, tale limite può essere efficacemente superato in via esegetica, attraverso il ricorso a principi contenuti in successivi documenti normativi ed è anche vero che tale criticità pone non poche questioni anche con riferimento alla tutela della proprietà intellettuale (cfr. il § 2.2). Ne consegue un forzato bilanciamento tra interessi diametralmente opposti da cui, come emergerà in seguito[332], dipenderà l'evoluzione applicativa delle decisioni automatizzate e il loro impatto sui diritti fondamentali.

L'art. 23, ponendosi come norma di chiusura, introduce poi la possibilità per gli Stati membri di circoscrivere la portata dei diritti poc'anzi descritti per poter salvaguardare un particolare interesse rilevante dell'Unione europea[333].

---

[329] Cfr. l'art. 9, § 2 lett. *a*).

[330] Per un approfondimento su questo punto B. Mittelstadt, L. Floridi, *The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts*, in *Science and Engineering Ethics 2016*, 22, pp. 303 e ss. e S. Watcher, B. Mittlestadt, L. Floridi, *Why a right to explanation of automated decision-making does not exist in the GDPR*, in *International Data Privacy Law*, vol. 7, 2017, pp. 76 e ss.

[331] Cfr. S. Wachter, B. Mittelstadt, L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017.

[332] Cfr. il § 2.2.

[333] In particolare, per una delle seguenti motivazioni « *a) national security; (b) defence; (c) public security; L 119/46 EN Official Journal of the European Union 4.5.2016 (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); (i) the protection of the data subject or the rights and freedoms of others; (j) the enforcement of civil law claims*». Art. 23, GDPR, cit.

La disciplina contenuta nell'art. 22 del GDPR sulle decisioni automatizzate va completata poi con la direttiva 2016/680/UE che[334], rispetto al citato regolamento - come visto già, peraltro, in precedenza[335]- costituisce una *lex specialis*, avente l'obiettivo di stabilire norme minime relative alla «protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica»[336]. Pertanto, tra i due strumenti normativi non vi è sovrapposizione dal momento che il primo esclude espressamente dal proprio ambito di applicazione il trattamento dei dati ai fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali[337].

Più nel dettaglio, anche l'art. 11 della direttiva prescrive il divieto per gli Stati membri di disporre decisioni basate unicamente su un trattamento automatizzato che produca effetti giuridici negativi o incida significativamente sui diritti fondamentali dell'interessato, salvo il caso in cui sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per il diritto di ottenere l'intervento umano da parte del titolare del trattamento[338]. Si tratta di una disposizione, come l'art. 22 GDPR, definita dalla dottrina piuttosto "ambigua"[339]: tutto sembra ruotare intorno all'esegesi dell'espressione "decisione basata unicamente su un trattamento automatizzato". A una prima lettura potrebbe trattarsi di un divieto, imposto dalla norma di decisioni nelle quali non vi sia alcun coinvolgimento umano nel processo decisionale[340]. La direttiva richiede come regola un intervento dell'uomo, con la specificazione che «per aversi un coinvolgimento umano,

[334] Come già visto nel cap. I, § 1, la direttiva 2016/680/UE del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla 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, nonché' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, è stata attuata in Italia con il d.lgs. 18 maggio 2018, n. 51. Il decreto regola il trattamento, interamente o parzialmente automatizzato dei dati personali per finalità di prevenzione e repressione dei reati, esecuzione di sanzioni penali, salvaguardia e prevenzione di minacce alla sicurezza pubblica (art. 1 c. 2), prevedendo un articolato sistema di garanzie (artt. 9-12) e di responsabilità in capo al titolare del trattamento (artt. 15, 16, 20), del responsabile del trattamento (art. 18) del responsabile della protezione dei dati (artt. 28, 30) e, infine, un articolato apparato sanzionatorio (artt. 37-46).

[335] Cfr. *supra* il cap. I, § 1.

[336] Cfr. l'art. 1, par. 1, direttiva 2016/680/UE.

[337] Cfr. il capitolo I, § 1.1.

[338] La direttiva, in ragione degli interessi pubblici alla prevenzione, indagine e repressione dei reati, non contempla il consenso esplicito dell'interessato come eccezione per l'utilizzo di un trattamento dei dati automatizzato. Neppure consente di rifiutare un trattamento che offra come garanzie il fondamento legislativo e la tutela dei diritti. Di converso, come poc'anzi accennato, attribuisce sempre il diritto ad ottenere l'intervento umano. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, p. 196.

[339] Cfr. M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra stati uniti ed Europa*, cit., p. 16.

[340] In tal senso, si veda il documento elaborato dal GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento* 2016/679, adottate il 3 ottobre 2017 e riviste il 6 febbraio 2018, p. 23, reperibili all'indirizzo https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (visualizzato in data 22.4.2021).

il titolare del trattamento deve garantire che qualsiasi controllo alla decisione sia significativo e non costituisca un semplice gesto simbolico»[341]. In altre parole, «*in order to escape the prohibition from Article 22 GDPR or Article 11 of the Directive on Data Protection in Criminal Matters, the human has to use the machine only as decision support, whereas the final decision is taken by the human*»[342].

Secondo parte della dottrina, posta anche la delicatezza del settore in cui si applica la direttiva, la norma pretenderebbe una lettura ancora più esigente, secondo la quale, al fine di garantire un intervento effettivo dell'uomo, la stessa decisione non potrebbe basarsi esclusivamente sull'*output* di un meccanismo automatizzato[343]. La disposizione, peraltro, ammette una deroga alla regola, a condizione che vi sia una previsione di tutele sufficienti per i diritti personali e che vi sia, quanto meno, un intervento umano. In questo senso, occorre che l'elemento cognitivo generato da un procedimento decisionale automatizzato sia confermato da altre fonti. Anche in questo caso, non è stata conferita una tutela espressa alla trasparenza del procedimento algoritmico, ma tale mancanza potrebbe essere superata laddove l'interessato eserciti il diritto di ottenere un intervento del giudice[344].

Inoltre, l'art. 11 non si limita a richiedere un intervento umano a fronte dell'utilizzo di strumenti in grado di disporre decisioni automatizzate, ma contiene significative indicazioni con riferimento alla tipologia di dati che possono – o meglio non possono – essere utilizzati per la profilazione[345]. Più nel dettaglio, il par. 2 fa espresso riferimento alle categorie particolari di dati personali, di cui all'art. 10, ossia quei dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché i dati genetici, quelli biometrici o relativi alla salute o, ancora, i dati relativi alla vita sessuale della persona o all'orientamento sessuale, che non possono essere impiegati per finalità di profilazione, a meno che non vi siano «misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato». Il par. 3 pone infine un divieto assoluto

[341] Cfr. sul punto le *Linee guida sul processo decisionale automatizzato*, cit., p. 23.

[342] Cfr. M. Brkan, *Do algoritms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond*, in *Electronic Journal*, gennaio 2017, p. 10, richiamato da M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra stati uniti ed Europa*, cit., p. 17.

[343] Cfr. A. Caia, *Commento all'art. 22 GDPR*, in AA.VV., *GDPR e normativa privacy. Commentario*, (a cura di) G.M. Riccio, G. Scorza, E. Belisario, Giuffrè, Milano, 2018, p. 227.

[344] Su questo punto, cfr. L. Pulito, *Il trattamento dei dati personali in ambito penale e l'uso del passenger name record per contrastare il terrorismo e altri reati gravi*, in *Processo penale e giustizia*, 2018, 6, p. 1148.

[345] La definizione di profilazione è fornita dall'art. 3, n. 4: «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica». Si tratta di una forma automatizzata di trattamento, effettuato su dati personali e finalizzato a valutare aspetti personali relativi a una persona fisica: viene impiegata per effettuare previsioni su persone usando dati provenienti da varie fonti per dedurre qualcosa su quella persona in base alle qualità di altre persone che appaiono statisticamente simili. Tre sono i momenti rilevanti: la raccolta dei dati; l'analisi automatizzata per individuare correlazioni; l'applicazione della correlazione a una persona fisica per effettuare previsioni su comportamenti futuri (*Linee guida sul processo decisionale automatizzato*, cit., pp. 7 e 8).

di profilazione basata sui dati appena richiamati che possa causare la discriminazione di persone fisiche.

Da questa prima ricostruzione normativa è possibile già scorgere un tentativo, a livello di Unione europea, di introdurre un primo "schema" base di regole, finalizzate alla salvaguardia del ruolo dell'intelligenza umana nei processi decisionali automatizzati e al divieto di utilizzo di *tools* basati sul trattamento di categorie di dati personali suscettibili di incidere sui diritti fondamentali degli interessati. Resta il fatto che, come già accennato *supra*, né il GDPR né la direttiva 2016/680/UE affrontano in modo diretto il tema dell'intelligenza artificiale e dei rischi per le sue diverse applicazioni in ambito giudiziario.

Bisogna attendere almeno il 2017, anno nel quale, sempre nell'ambito dell'Unione europea, si è cominciato apertamente ad aprire il dibattito sull'IA, tramite la Risoluzione del Parlamento europeo sulla robotica[346], che annunciava la nascita di robot intelligenti autonomi ed evocava la necessità di attribuire diritti e doveri a queste nuove entità giuridiche. Nello stesso atto è previsto un invito espresso, formulato nei confronti della Commissione europea, a considerare concretamente l'idea della creazione di un'agenzia per l'intelligenza artificiale e a definire un quadro politico globale, al fine di mitigare i rischi di potenziali violazioni di diritti fondamentali.

Nel marzo del 2018, questa volta nell'ambito del Consiglio d'Europa, è stato pubblicato l'interessante studio dal titolo "*Algorithms and Human Rights*"[347], nella cui sezione dedicata al *fair trial* e al *due process* si anticipavano alcune delle preoccupazioni affrontate poi a distanza di qualche mese dalla "Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia". In particolare, con tale documento cominciano a diffondersi diverse riflessioni sulla tenuta dei principi della presunzione di innocenza, della parità delle armi e del contraddittorio. Il rischio è che sistemi algoritmici possano essere impropriamente impiegati dai giudici per delegare la decisione a strumenti tecnologici non adeguati a tale scopo[348].

Circa un mese dopo, con la Comunicazione COM(2018) 237 final[349] - "*L'intelligenza artificiale per l'Europa*", la Commissione europea esordiva affermando che «*artificial intelligence (AI) is*

---

[346] PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica* (2015/2103(INL)), v. https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A52017IP0051 (visualizzato in data 22.4.2021).

[347] Reperibile all'indirizzo https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5 (visualizzato in data 13.5.2021).

[348] Cfr. COMMITTEE OF EXPERT OF INTERNET INTERMEDIARIES, *Algorithms and Human Rights*, cit., p. 12: «*Given the pressure of high caseloads and insufficient resources from which most judiciaries suffer, there is a danger that support systems based on artificial intelligence are inappropriately used by judges to «delegate» decisions to technological systems that were not developed for that purpose and are perceived as being more «objective» even when this is not the case. Great care should therefore be taken to assess what such systems can deliver and under what conditions that may be used in order not to jeopardise the right to a fair trial*».

[349] Comunicazione COM(2018) 237 final – "*L'intelligenza artificiale per l'Europa*". Il testo è reperibile su https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52018DC0237 (visualizzato in data 22.4.2021).

already part of our lives – it is not science fiction». In questa occasione, il messaggio fondamentale che la Commissione ha inteso diffondere è che sussiste «*the need to join forces at European level, to ensure that all Europeans are part of the digital transformation, that adequate resources are devoted to AI and that the Union's values and fundamental rights are at the forefront of the AI landscape*». L'impegno di fondo si snoda in due obiettivi distinti fondamentali: portare gli investimenti economici in questo ambito ad un livello più alto e garantire che le nuove tecnologie riflettano i "valori" fondamentali europei. Riguardo a questi, con la Comunicazione, la Commissione europea ha preannunciato l'elaborazione di una serie di linee guida etiche per la regolamentazione dell'IA da parte di un gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale, istituito dalla Commissione europea nel giugno 2018[350]. Di lì, per la prima volta, è stato introdotto il concetto di "intelligenza artificiale affidabile", conforme alla normativa e etica, oltre che "robusta" in termini di sicurezza, protezione e affidabilità. A tal proposito, qualsiasi approccio "umanocentrico" all'IA richiede il rispetto rigoroso dei diritti fondamentali[351]. Viene ribadito, poi, l'impegno dell'Unione europea a non produrre nuove forme di disuguaglianze, specialmente riferite a certe categorie di popolazione, ossia a "lavoratori, donne, persone con disabilità, minoranze etniche, bambini, consumatori o altri a rischio di esclusione". Le linee guida hanno poi identificato quattro principi chiave, definiti "*imperatives*", per un'IA affidabile: il rispetto dell'autonomia umana, la prevenzione del danno, l'equità e l'esplicabilità, intesa come trasparenza e tracciabilità delle informazioni e del procedimento seguito dai sistemi di intelligenza artificiale[352].

L'8 aprile 2019, con la pubblicazione delle *Ethics guidelines for trustworthy AI*, l'Unione europea ha introdotto un tassello ulteriore, ossia la concezione secondo la quale la necessità di un'IA affidabile non debba essere considerata un obiettivo da raggiungere, ma il fondamento stesso di un sistema normativo completamente nuovo, le cui applicazioni potenzialmente più lesive dei diritti fondamentali debbano sempre essere soggette ad una valutazione obbligatoria. Queste ultime includono la sorveglianza di massa e l'uso delle cd. "armi autonome"[353]. Con specifico riferimento al primo fenomeno, le *Guidelines* raccomandano alle autorità degli Stati membri di emanare atti che garantiscano l'individuo da attività di «*identifying and tracking*», attraverso sistemi di riconoscimento biometrico basati sull'intelligenza artificiale come i «*face recognition and other involuntary methods of identification using biometric data (i.e. lie detection, personality assessment through micro*

[350] *Ethics guidelines for trustworthy AI*, reperibili su https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (visualizzato in data 22.4.2021).
[351] Per es. nel Trattato sull'Unione europea (TUE) o la Carta dei Diritti Fondamentali dell'Unione europea.
[352] Cfr. *Ethics guidelines for trustworthy AI*, cit., p. 10.
[353] Cfr. *Ethics guidelines for trustworthy AI*, cit., p. 34.

expressions, and automatic voice detection)»[354]. L'utilizzo di tali strumenti dovrebbe essere consentito solo in circostanze eccezionali, come per esempio in caso di minacce per la sicurezza nazionale, ma comunque anche in tali occasioni l'impiego è autorizzato solo se basato sul rispetto dei diritti fondamentali[355]. Tale indirizzo ermeneutico è lo stesso che sembra muovere il Consiglio dell'Unione europea che, nelle conclusioni sul piano coordinato per lo sviluppo e l'uso dell'IA[356] elaborato dalla Commissione europea[357], ha posto in luce la necessità di garantire un utilizzo dei nuovi sistemi di IA nel rispetto dei valori dell'Unione europea e dei diritti fondamentali dell'uomo.

Quasi contestualmente, nell'ambito del Consiglio d'Europa, si colloca l'adozione da parte della Commissione europea per l'efficienza della giustizia (CEPEJ) della "Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia" e dei principi in essa enunciati[358], nel cui Preambolo i legislatori nazionali sono stati invitati a «stabilire una cornice normativa entro la quale i nuovi strumenti vadano sviluppati, verificati e utilizzati» e a disporre di un elenco di valori ineludibili per aderire a una forma di intelligenza artificiale che aspiri a porsi come «antropocentrica e affidabile». Il documento è rivolto principalmente ai «*public and private stakeholders responsible for the design and deployment of artificial intelligence tools and services that involve the processing of judicial decisions and data*», nonchè ai «*public-decision makers in charge of the legislative or regulatory framework, of the development, audit or use of such tools and services*»[359]. Trattasi di un significativo documento di *soft law* che muove dalla consapevolezza che l'IA sia in grado di generare enormi vantaggi per gli individui e per la società, ma porti con sé anche determinati rischi che vanno gestiti

[354] Cfr. *Ethics guidelines for trustworthy AI*, cit., p. 33.

[355] «*AI enables the ever more efficient identification of individual persons by both public and private entities. Noteworthy examples of a scalable AI identification technology are face recognition and other involuntary methods of identification using biometric data (i.e. lie detection, personality assessment through micro expressions, and automatic voice detection). Identification of individuals is sometimes the desirable outcome, aligned with ethical principles (for example in detecting fraud, money laundering, or terrorist financing). However, automatic identification raises strong concerns of both a legal and ethical nature, as it may have an unexpected impact on many psychological and sociocultural levels. A proportionate use of control techniques in AI is needed to uphold the autonomy of European citizens. Clearly defining if, when and how AI can be used for automated identification of individuals and differentiating between the identification of an individual vs the tracing and tracking of an individual, and between targeted surveillance and mass surveillance, will be crucial for the achievement of Trustworthy AI. The application of such technologies must be clearly warranted in existing law. Where the legal basis for such activity is "consent", practical means must be developed which allow meaningful and verified consent to be given to being automatically identified by AI or equivalent technologies. This also applies to the usage of "anonymous" personal data that can be re-personalised*». Cfr. *Ethics guidelines for trustworthy AI*, cit., pp. 33-34.

[356] Le conclusioni del Consiglio dell'Unione europea sono reperibili all'indirizzo https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/it/pdf (visualizzato in data 22.4.2021).

[357] Il documento è reperibile all'indirizzo https://data.consilium.europa.eu/doc/document/ST-15641-2018-INIT/en/pdf (visualizzato in data 22.4.2021).

[358] Cfr. CEPEJ - *European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment*, reperibile su https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment (visualizzato in data 22.4.2021).

[359] Cfr. CEPEJ - *European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment*, cit., p. 5.

in modo adeguato. In tale ottica si afferma la necessità di assicurare che «*AI is human-centric: AI should be developed, deployed and used with an "ethical purpose" (...), grounded in and reflective of fundamental rights, societal values and the ethical principles of Beneficence (do good), Non-Maleficence (do no harm), Autonomy of humans, Justice, and Explicability*»[360]. Ne deriva un approccio completamente antropocentrico all'intelligenza artificiale che postula il rispetto della dignità e dell'autonomia delle persone, alle quali va sempre garantito un potere di supervisione sulle macchine[361]. Più nel dettaglio, come si avrà modo di approfondire *infra* (cfr. il § 2.2), i principali obiettivi sono il rispetto dei diritti fondamentali nella progettazione e nell'applicazione di sistemi di intelligenza artificiale, il divieto di discriminazione legata al rischio di immissione di *input* non neutri, una garanzia di qualità e di sicurezza dei dati e delle decisioni giudiziarie da utilizzare per l'elaborazione mediante sistemi computazionali, solo se integri, intangibili e provenienti da fonti affidabili, una garanzia di trasparenza, imparzialità e *fairness* in modo da assicurare, tramite i requisiti di accessibilità, comprensibilità e verificabilità esterna dei processi computazionali relativi all'analisi dei dati giudiziari; infine, la facoltà di controllo da parte dell'utente. Un *focus* particolare è stato poi posto sul divieto di decisioni basate unicamente su un trattamento automatizzato che ha suggerito in dottrina «gli spunti per un'urgente discussione tra scienze penali e informatiche»[362].

In una prospettiva più "politica", prosegue l'azione dell'Unione europea con il «*Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*» del 19 febbraio 2020, tramite il quale, adottando un approccio normativo basato sul rischio di potenziale lesione dei diritti fondamentali, la Commissione europea ha espresso il duplice obiettivo di promuovere l'adozione dell'IA e di affrontare i rischi - quali meccanismi decisionali opachi, discriminazioni basate sul genere o di altro tipo, intrusioni nella vita privata degli individui o utilizzi per scopi criminali - al fine di definire le opzioni strategiche su come raggiungere gli stessi[363]. L'approccio basato sul rischio sembra offrire il concreto vantaggio di poter adattare la specifica norma alla rilevanza degli interessi giuridici coinvolti, al potenziale danno previsto e all'evitabilità dei rischi da parte delle persone interessate. Comincia a profilarsi la possibilità di introdurre delle vere e proprie classi di rischio rispetto ai diversi sistemi di IA, che troveranno poi espressa previsione solo con la recente proposta di regolamento (cfr. *infra* il § successivo). Il *White Paper*, definendo le specifiche opzioni politiche

[360] Così, *Ethics Guidelines*, cit., p. 13.

[361] Su questo punto v. M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, cit., p. 15.

[362] Cfr. S. Quattrocolo, *Intelligenza artificiale e giustizia nella cornice della Carta etica europea. Gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *www.lalegislazionepenale.it*, 2018.

[363] Cfr. COMMISSIONE EUROPEA [COM (2020,) 65 final], *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, consultabile sul sito internet della Commissione (ultimo accesso il 5 ottobre 2020). Esso è espressamente condiviso dalle *Conclusioni del Consiglio dell'Unione Europea*, "Accesso alla giustizia – Cogliere le opportunità della digitalizzazione", in G.U.U.E., 14.10.2020 n. C 342, n. 42 ss., p. I/6.

su come ottenere lo scopo predetto, parte dal presupposto per cui il rapido sviluppo dell'intelligenza artificiale ha determinato profondi cambiamenti nei modelli di produzione e di erogazione di servizi, migliorando l'assistenza sanitaria, aumentando l'efficienza dell'agricoltura, contribuendo alla mitigazione dei cambiamenti climatici e all'adattamento ai medesimi, migliorando l'efficienza dei sistemi di produzione e aumentando generalmente la sicurezza dei cittadini europei. In tal senso, la Commissione europea raccomanda agli Stati e alle istituzioni europee l'elaborazione di strategie comuni e unitarie per affrontare l'attuale trasformazione e le sfide del futuro con maggiore consapevolezza e responsabilità.

Sono seguite, poi, le più recenti conclusioni del Consiglio dell'Unione europea, nelle quali sono state poste in luce l'opacità, la complessità, la distorsione e un certo grado di imprevedibilità in alcuni comportamenti definiti "parzialmente autonomi" di determinati sistemi di IA, al fine di denunciare la loro attuale incompatibilità con i diritti fondamentali e facilitare l'introduzione di norme giuridiche[364]. Invero, sulla scia tracciata dalle conclusioni del Consiglio dell'Unione europea, il Parlamento ha adottato una serie di risoluzioni concernenti l'utilizzo dell'IA, riguardo, in particolare, all'etica[365], alla responsabilità[366] e in materia di *copyright*[367]. A queste sono seguite le risoluzioni sull'IA in materia penale[368] e nel settore dell'istruzione, della cultura e dell'audiovisivo[369]. Peraltro, in occasione della risoluzione sull'IA in materia penale, la Commissione per le libertà civili, la giustizia e gli affari interni ha chiesto espressamente una moratoria sulla diffusione dei sistemi di riconoscimento facciale a fini di contrasto e repressione dei reati nello spazio euro-unitario, affermando che «l'attuale stato di avanzamento di tali tecnologie e il loro impatto significativo sui diritti fondamentali richiedono un dibattito sociale aperto e approfondito, al fine di esaminare le diverse problematiche sollevate e la giustificazione di una loro diffusione»[370].

Infine, di particolare interesse è la Risoluzione del Parlamento europeo che ha ribadito il suo impegno a garantire il rispetto di una serie di principi etici per lo sviluppo, l'introduzione e l'uso dell'IA, della robotica e delle tecnologie correlate, facendo propri i valori già richiamati nell'ambito

---

[364] Cfr. CONSIGLIO DELL'UNIONE EUROPEA, *Conclusioni della Presidenza - La Carta dei diritti fondamentali nel contesto dell'intelligenza artificiale e del cambiamento digitale*, 11481/20, 2020.

[365] Cfr. *Risoluzione del Parlamento europeo del 20 ottobre 2020 su un quadro degli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate*, 2020/2012(INL).

[366] Cfr. *Risoluzione del Parlamento europeo del 20 ottobre 2020 su un regime di responsabilità civile per l'intelligenza artificiale*, 2020/2014(INL).

[367] Cfr. *Risoluzione del Parlamento europeo del 20 ottobre 2020 sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale*, 2020/2015(INI).

[368] Cfr. *Progetto di relazione del Parlamento europeo, Intelligenza artificiale nel diritto penale e suo utilizzo da parte della polizia e delle autorità giudiziarie in materia penale*, 2020/2016(INI).

[369] Cfr. 2020/2017(INI).

[370] Cfr. *Progetto di relazione del Parlamento europeo, Intelligenza artificiale nel diritto penale e suo utilizzo da parte della polizia e delle autorità giudiziarie in materia penale*, cit., p. 9.

del Consiglio d'Europa dalla CEPEJ nella "*Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia*" (cfr. *supra*)[371].

Insomma, sembra che sia il Consiglio d'Europa sia l'Unione europea abbiano mosso quasi contestualmente i primi passi nell'implementazione di un quadro giuridico idoneo, per un consapevole utilizzo dell'intelligenza artificiale, condividendo gli stessi obiettivi volti a promuovere l'eccellenza nell'IA e i valori finalizzati a garantire una tecnologia affidabile.

2.1.1. La proposta di regolamento europeo sull'intelligenza artificiale 2021/0106(COD)

Entro tale scenario, in data 21 aprile 2021 si colloca cronologicamente la pubblicazione di una proposta di regolamento da parte della Commissione europea «*on a European approach for Artificial Intelligence*» *(Artificial Intelligence Act)*, le cui norme, dopo il consueto *iter* procedimentale di emanazione, saranno applicabili direttamente in ciascuno Stato membro[372]. Il documento ribadisce i valori fondamentali a cui è ispirata l'azione dell'UE e mira a dare agli utenti la fiducia necessaria per servirsi di strumenti basati sull'IA, incoraggiando al contempo le imprese a svilupparli[373].

A partire dalla relazione alla proposta di regolamento (*explanatory memorandum*)[374], la Commissione europea ha svolto un approfondito *excursus* sugli elementi storico-giuridici che hanno spinto sempre di più verso una concreta esigenza di adottare un testo che potesse dettare alcuni standard minimi nel procedimento di elaborazione dei dati da parte dei sistemi di intelligenza artificiale. Come visto, lo sviluppo e la diffusione di strumenti di IA ha portato numerosi benefici sia economici che sociali nel panorama industriale e in generale nelle attività sociali[375]. Migliorando e

---

[371] Cfr. *Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale*, 2020/2016(INI).

[372] Cfr. EUROPEAN COMMISSION, *Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts*, COM(2021) 206 final, reperibile all'indirizzo https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence (visualizzato in data 23.4.2021), accompagnato da un nuovo piano coordinato sull'intelligenza artificiale 2021, reperibile su https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review (visualizzato in data 26.4.20219. Nella stessa occasione, unitamente alla proposta di regolamento sulle applicazioni di AI e al Piano di coordinamento 2021, la Commissione europea ha presentato anche la bozza di regolamento sui robot (*machinery products*), COM (2021) 202, destinato a sostituire la Direttiva (EU) 2006/42/EC (*Machinery Directive*), reperibile su https://ec.europa.eu/docsroom/documents/45508 (visualizzato in data 26.4.2021).

[373] Cfr. G. De Gregorio, *The Digital Services Act: A Paradigmatic Example of European Digital Constitutionalism*, in *Diritti Comparati*, 17.5.2021, pp. 1, M. Ebers, V.R.S. Hoch, F. Rosenkranz, H. Ruschemeier, B. Steinrötter, *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society*, in *(RAILS). J.* 2021, 4(4), pp. 589-603, L. Floridi, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in *Philos. Technol*. 34, 2021, pp. 215–222, M. Hildebrandt, *The Proposal for an EU AI Act of 21 April 2021*, in *Brief Commentary*, 2021, reperibile all'indirizzo https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legalrequirements/F2662611_en (visualizzato in data 29.9.2021).

[374] Cfr. EUROPEAN COMMISSION, *Proposal for a* Regulation, cit., pp. 1-16.

[375] Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation*, cit., p. 1.

ottimizzando «*the free movement of AI-based goods and services cross-border*», l'uso dell'IA è in grado di fornire vantaggi competitivi alle aziende e supportare così il raggiungimento di obiettivi socialmente e ambientalmente vantaggiosi in diversi settori[376]. L'altro lato della medaglia è rappresentato dalla possibilità che la fruizione di talune applicazioni dei sistemi di intelligenza artificiale possa talora causare addirittura dei danni, sia materiali sia immateriali, ai singoli individui, «*to the health and safety or fundamental rights*»[377]. Ne consegue la necessità di istituire un quadro giuridico che ponga «*harmonised rules on artificial intelligence (…) therefore needed to foster the development, use and uptake of artificial intelligence in the internal market that at the same time meets a high level of protection of public interests*»[378]. In tal modo, l'introduzione di requisiti minimi di qualità e di sicurezza consentirà un generale miglioramento del funzionamento del mercato interno con la creazione delle condizioni per lo sviluppo di un vero e proprio "ecosistema" di fiducia che copra l'intero processo di produzione, commercializzazione, vendita e utilizzo dell'intelligenza artificiale all'interno dell'Unione europea.

L'approccio che guida l'intera bozza di regolamento è quello del "rischio" di lesività dei diritti fondamentali degli individui, già presente, ma diversamente declinato nel precedente *White Paper* (cfr. *supra* il § 2)[379]. La bozza di regolamento parte dal presupposto che, mentre alcuni sistemi di IA ritenuti "a rischio inaccettabile" dovrebbero essere vietati[380], altri, rientranti nella categoria "ad alto

---

[376] Quali quelli sanitario, agricolo, educativo, della gestione delle infrastrutture, dell'energia, dei trasporti, della logistica, dei servizi pubblici, della sicurezza e della mitigazione e adattamento ai cambiamenti climatici. EUROPEAN COMMISSION, *Proposal for a Regulation,* cit., p. 18.

[377] Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation,* cit., p. 3.

[378] Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation,* cit., p. 18.

[379] Sono individuati diversi livelli di rischio: minimo, basso, alto e inaccettabile. Mentre le applicazioni a rischio "inaccettabile" sono inderogabilmente vietate dall'Unione europea, quelle ad "alto rischio" sono consentite se sono rispettati i requisiti introdotti dalla bozza di regolamento, tra i quali figurano il rispetto di adeguati sistemi di valutazione e attenuazione dei rischi, un'elevata qualità dei *set* di dati immessi nel sistema, al fine di ridurre il più possibile i rischi e i risultati discriminatori, una puntuale documentazione delle attività compiute per garantire la tracciabilità dei risultati, delle informazioni chiare e adeguate per l'utente, una costante supervisione umana e un elevato grado di robustezza, sicurezza e accuratezza dei sistemi di IA. È interessante notare che tra i sistemi ad alto rischio che devono rispettare tutta questa serie di requisiti figurano altresì gli «*AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons*» [cfr. ANNEXES to the *Proposal for a Regulation of the European Parliament and of the Council Laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts* reperibile all'indirizzo https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence (visualizzato il 29.4.2021)]. I sistemi di riconoscimento biometrico in entrambe le modalità sono quindi considerati ad "alto rischio". Tra gli strumenti a "basso rischio", invece, la bozza di regolamento annovera i «*chatbots or 'deep fakes'*», per i quali sono previsti «*only minimum transparency obligations*». In questi casi, per esempio, sarà necessario rendere esplicito all'utente che la sua interfaccia è un sistema operativo non umano. I *tools* a rischio minimo, invece, sarebbero sempre consentiti. EUROPEAN COMMISSION, *Proposal for a Regulation,* cit., pp. 3 e ss.

[380] Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation*, cit., pp. 12 e 13: «*the prohibitions covers practices that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness or exploit EN 13 EN vulnerabilities of specific vulnerable groups such as children or persons with disabilities in order to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm. Other manipulative or exploitative practices affecting adults that might be facilitated by AI systems could be covered by the existing data protection, consumer protection and digital service legislation that guarantee that natural persons are properly informed and have free choice*

rischio" dovrebbero essere sottoposti a requisiti prescrittivi, tecnicamente anche molto dettagliati, che, a tratti, evocano l'impianto normativo del GDPR (già richiamato *supra*, nel capitolo I, § 1 e nel capitolo II, al paragrafo precedente)[381]. In particolare, i profili caratterizzanti la proposta sono: precise regole sulla valutazione d'impatto, l'inserimento nei sistemi di IA di dati caratterizzati da alti livelli di qualità, la tracciabilità dei risultati, una costante supervisione umana nell'utilizzo di tali sistemi, un alto livello di robustezza, sicurezza e accuratezza generale[382].

Risulta peraltro interessante soffermarsi sui principali punti di contatto che la proposta di regolamento mostra proprio con il già più volte richiamato GDPR. Una prima assonanza può intuirsi già a partire dalle definizioni: come descritto nel capitolo I, § 1 analogamente a quanto definito dall'art. 4(14) GDPR con riferimento alla nozione di "dato biometrico", la proposta di regolamento li definisce come «*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*»[383]. Il documento aggiunge un tassello ulteriore rispetto alla definizione riportata nel GDPR: la proposta infatti prosegue definendo cosa possa, a sua volta, essere qualificato come un "sistema di identificazione biometrica da remoto", specificando che esso costituisce uno strumento avente lo scopo di riconoscere le persone a distanza sulla base dei loro dati biometrici, contenuti in un archivio digitale di riferimento, relativi

not to be subject to profiling or other practices that might affect their behaviour. The proposal also prohibits AI-based social scoring for general purposes done by public authorities. Finally, the use of 'real time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is also prohibited unless certain limited exceptions apply».

[381] Cfr. 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, che abroga la direttiva 95/46/CE (Cfr. il capitolo I, §§ 1 e 1.1, supra il § 2.1), reperibile su https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016R0679 (ultimo accesso in data 26.4.2021).

[382] Sono considerate applicazioni ad "alto rischio" i sistemi usati per determinare l'accesso a istituzioni educative o di formazione, o per valutare gli studenti, l'applicazione di IA nella chirurgia assistita da robot, i sistemi usati per lo *screening* o il filtraggio delle candidature di lavoro, i sistemi per valutare l'affidabilità creditizia delle persone, i sistemi di valutazione dell'affidabilità delle informazioni fornite da persone fisiche per prevenire, investigare o prevenire reati, i sistemi per il trattamento e l'esame delle domande di asilo e visto e i sistemi per assistere i giudici in tribunale. La proposta di regolamento specifica che «*the proposed rules will be enforced through a governance system at Member States level, building on already existing structures, and a cooperation mechanism at Union level with the establishment of a European Artificial Intelligence Board*». EUROPEAN COMMISSION, *Proposal for a Regulation,* cit., p. 3.

[383] Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation,* cit., art. 3, pt. 33. Come ricordato *supra* al capitolo I, § 1, il Consiglio dell'Unione europea, nel primo testo di modifica delle disposizioni contenute nella proposta diffuso di recente, ha proposto di eliminare l'espressione «*which allow or confirm the unique identification of that natural person*». Cfr. COUNCIL OF THE EUROPEAN UNION, *Presidency compromise text*, 2021/0106(COD), 29.11.2021, reperibile all'indirizzo https://media-exp1.licdn.com/dms/document/C4D1FAQGuV1FL6qMDIA/feedshare-document-pdf-analyzed, (visualizzato in data 13.12.2021). Il Parlamento europeo, tramite il COMMITTEE ON LEGAL AFFAIRS FOR THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION AND THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft Opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts* (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 2.3.2022 ha successivamente proposto di emendare la definizione come segue «*personal data resulting from specific technical processing relating to the physical, or physiological or behavioural characteristics of a natural person, which confirm the unique identification of that natural person, such as dactyloscopic data*».

alle caratteristiche fisiche o comportamentali di un individuo che ne consentono o confermano l'identificazione univoca, senza che l'utente ne sia a conoscenza[384]. Sul piano tassonomico, dunque, la bozza di regolamento compie un ulteriore sforzo rispetto al GDPR. Tuttavia, la proposta ripete le stesse espressioni, già non esenti da critiche rispetto al testo del regolamento (UE) 2016/679 (cfr. il capitolo I, § 1).

Parimenti poi con quanto previsto dal Regolamento GDPR[385], in capo al produttore del sistema di intelligenza artificiale si pone l'onere di svolgere un cd. "*conformity assessment*", prima che il prodotto sia messo in commercio, che dimostri che i requisiti del regolamento siano stati rispettati. Proprio riguardo alla valutazione del rischio, sembrano esserci i più rilevanti punti di contatto tra la bozza di regolamento e la disciplina sulla tutela dei dati personali: infatti, alla luce del particolare impatto che ciascun sistema di intelligenza artificiale potrebbe avere nei confronti dei diritti fondamentali dell'individuo, è stato stabilito un livello di rischio che però, contrariamente a quanto avviene nel GDPR, potrebbe essere neutralizzato attraverso il rispetto di specifici requisiti, elencati dagli artt. 6 e ss. della proposta di regolamento. Più nel dettaglio, ai sensi dell'art. 9, è prevista l'implementazione di un sistema di gestione del rischio, anch'esso documentale e periodicamente monitorato, in relazione al variare del pericolo connesso all'utilizzo dei vari sistemi di intelligenza artificiale[386]. Un aspetto particolarmente rilevante è rappresentato dalla pretesa qualità dei dati immessi nel sistema durante la fase di sviluppo e di *testing* del software: essi devono essere pertinenti,

[384] L'aggettivo "*remote*" viene pertanto impiegato per indicare i sistemi che non richiedono un contatto diretto con un sensore per eseguire il riconoscimento. Giova sottolineare che il Consiglio dell'Unione europea, nel primo testo di modifica delle disposizioni contenute nella proposta diffuso di recente, ha proposto di eliminare dalla definizione dei sistemi di riconoscimento biometrico l'aggettivo "*remote*" per includere qualsiasi «*AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database data repository, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used*» (v. considerando n. 8). Cfr. COUNCIL OF THE EUROPEAN UNION, *Presidency compromise text*, 2021/0106(COD), 29.11.2021, reperibile all'indirizzo https://media-exp1.licdn.com/dms/document/C4D1FAQGuV1FL6qMDIA/feedshare-document-pdf-analyzed, (visualizzato in data 13.12.2021). Il Parlamento europeo, tramite il COMMITTEE ON LEGAL AFFAIRS FOR THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION AND THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft Opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts* (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 2.3.2022, p. 8, ha proposto di specificare che «*the notion of remote biometric identification system should not cover AI systems, which allow for an identification of a natural person, such as door locks, security systems etc*.» (considerando n. 8).

[385] Il principale strumento di *assessment* è rappresentato dal Registro delle attività di trattamento e dallo svolgimento di idonee valutazioni del rischio che il trattamento stesso può comportare nei confronti dell'interessato. Cfr. l'art. 35 GDPR.

[386] Esso comprende le seguenti fasi: «*(a) identification and analysis of the known and foreseeable risks associated with each high-risk AI system; (b) estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse; (c) evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61; (d) adoption of suitable risk management measures in accordance with the provisions of the following paragraphs*». EUROPEAN COMMISSION, *Proposal for a Regulation*, cit., art. 9, par. 2.

liberi da errori e completi[387]. Tale disposizione era già presente nel testo del GDPR: i dati trattati devono essere caratterizzati da particolari elementi che ne attestino la qualità, tra cui l'adeguatezza, la pertinenza, l'esattezza e, se necessario, il periodico aggiornamento (art. 5)[388]. A questo punto, in un'ottica di pura "*accountability*", i risultati elaborati dovranno essere verificati e sistematicamente monitorati lungo l'intero arco di vita del sistema. Tuttavia, a fronte della predisposizione di una serie di requisiti tecnici anche molto dettagliati, ai quali i sistemi di IA devono risultare conformi, la proposta non introduce analoghi strumenti sanzionatori per punire eventuali trasgressioni e individuare specificamente i responsabili. Il rischio che si corre è quello di considerare un sistema di autovalutazione tecnico eseguito dai fornitori di IA come una garanzia effettiva contro i pericoli che tali tecnologie possono generare per i diritti fondamentali (cfr. *infra* il § 3.1).

L'art. 62, in analogia con quanto statuito nel GDPR[389], prevede comunque l'obbligo per i fornitori dei sistemi di IA ad "alto rischio" di notificare alle Autorità competenti nazionali ogni eventuale incidente o malfunzionamento dello strumento che possa costituire una "violazione" degli obblighi previsti dal diritto dell'Unione, volti a tutelare i diritti fondamentali degli Stati membri in cui si è verificato l'incidente o la violazione[390].

Venendo alla trattazione di una delle norme "cardine" del futuro quadro giuridico ai sensi dell'art. 5 della proposta, si rileva che è stato posto il divieto di impiego di talune pratiche di intelligenza artificiale, tra cui la messa a disposizione o l'utilizzo di un sistema che, sfruttando «*subliminal techniques beyond a person's consciousness*»[391], sia in grado di alterare materialmente il comportamento in modo da causare, o rendere probabile la determinazione di un danno fisico o psicologico ad un soggetto. Alla lettera *b*) dello stesso articolo sono richiamate le tecniche di IA che sfruttano una qualsiasi delle «*vulnerabilities*» di uno specifico gruppo di persone a causa della loro

---

[387] Il Parlamento europeo, tramite il COMMITTEE ON LEGAL AFFAIRS FOR THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION AND THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft Opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, cit., p. 56, ha specificato che «*in assessing the quality of a data set, account shall be taken to the extent to which the data set is constructed with a view to fulfilling in particular the following aspects: a) provides a similar output for relevant demographic Groups impacted by the system; b) minimizes disparities in outcomes for relevant demographic groups impacted by the system, in case where the system allocates resources or opportunities to natural persons; c) minimizes the potential for stereotyping, demeaning, or erasing relevant demographic groups impacted by the system where the system describes, depicts, or otherwise represents people, cultures, or society*» (art. 10, par. 3).

[388] Trattasi di una prescrizione già presente nella Direttiva 95/46/CE del 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[389] Cfr. l'art. 33 GDPR.

[390] Più nel dettaglio, «*such notification shall be made immediately after the provider has established a causal link between the AI system and the incident or malfunctioning or the reasonable likelihood of such a link, and, in any event, not later than 15 days after the providers becomes aware of the serious incident or of the malfunctioning*». EUROPEAN COMMISSION, *Proposal for a Regulation*, cit., art. 62. Con riferimento alle sanzioni, invece, la proposta di regolamento appare ancora più afflittiva rispetto al GDPR: fino al 6% del fatturato globale (contro il 4% del GDPR).

[391] Potrebbe essere utile definire tali pratiche in modo tale da riconoscere più facilmente determinate attività abusive.

età e disabilità fisica o mentale, «*in order to materially distort the behaviour of a person pertaining to that group in a manner*» e da che ne possa derivare un danno fisico e psicologico. Lo scopo della disposizione risulta piuttosto evidente: proteggere determinate categorie di individui da usi completamente distorti di tali tecniche di IA. La stessa norma prosegue facendo divieto alle autorità pubbliche di utilizzare sistemi di IA per valutare o classificare l'affidabilità delle persone fisiche per un certo periodo di tempo, in base al loro comportamento usuale o ad altre caratteristiche personali note o previste, con l'assegnazione di un "*social scoring*" (lett. *c*)[392]. Come si approfondirà meglio *infra*, al par. 3, la lett. *d*) dispone il divieto di impiego di sistemi di identificazione biometrica "in tempo reale" o "contestuale" (cfr. il cap. I, § 1.1) in spazi aperti al pubblico[393], da parte delle autorità di *law enforcement*, a meno che e nella misura in cui tale uso sia strettamente necessario per il perseguimento di uno dei seguenti obiettivi: «*(i) the targeted search for specific potential victims of crime, including missing children; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State*»[394]. Mentre l'ambito di operatività dell'ultimo obiettivo risulta piuttosto circoscritto, le prime due categorie appaiono caratterizzate da contorni alquanto sfumati. Con quali modalità e a fronte di quali specifiche circostanze fattuali le autorità di polizia giudiziaria sono autorizzate ad eseguire ricerche mirate di "potenziali" vittime di reato? Quale univoca definizione può essere data ad una "vittima potenziale" di reato per evitare che venga effettuato un uso distorto della tecnologia e si collezionino dati di individui del tutto estranei a qualsivoglia fattispecie di reato?[395] Ancora, oltre ai caratteri di "specificità, sostanzialità e imminenza", quali altri requisiti deve rispettare una minaccia che a priori appaia alle autorità di *law enforcement* in grado di attentare alla vita o alla sicurezza pubblica, al fine di poter utilizzare tali tecniche di identificazione?

[392] La disposizione mira a prevenire il verificarsi di due possibili conseguenze: «*(i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected; (ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity*;». EUROPEAN COMMISSION, *Proposal for a Regulation*, cit., art. 5, lett. *c*), pt. i) e ii).

[393] Con riferimento alla modalità "*real time*" del software di riconoscimento facciale italiano si dirà meglio *infra*, al capitolo IV, § 1.3. Si sottolinea che l'elemento che differenzia un sistema biometrico *real time* ad "alto rischio" e un sistema biometrico *real time* a rischio inaccettabile e, quindi, vietato è il contesto entro cui lo strumento viene utilizzato.

[394] Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation*, cit., art. 5, lett. *d*).

[395] A tal proposito, anche la direttiva 2012/29/UE del Parlamento europeo e del Consiglio del 25.10.2012 che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato e che sostituisce la decisione quadro 2001/220/GAI, non fornisce una definizione dell'espressione.

Con riferimento alla lett. *d*), si rileva l'ulteriore prescrizione di un'autorizzazione all'utilizzo di tali sistemi di identificazione biometrica "*real time*" concessa da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'utilizzo, rilasciata su richiesta motivata e conformemente alle norme dettate dal diritto nazionale dello Stato membro interessato[396]. È previsto che l'autorità giudiziaria o amministrativa competente, al fine di rilasciare l'autorizzazione, proceda alla valutazione degli elementi presentati dal richiedente[397], affinché stabilisca se l'impiego del sistema di identificazione biometrica considerato sia o meno necessario e proporzionato al conseguimento di uno degli obiettivi indicati dall'art. 5, par. 3, lett. *d*).

Sulle diverse perplessità che sorgono a una prima lettura dell'intera disposizione si avrà più ampiamente modo di tornare in seguito.

Un'altra previsione di particolare interesse all'interno della proposta è l'art. 13, che introduce precisi obblighi di *transparency* sul funzionamento dei sistemi di intelligenza artificiale non solo nei confronti dell'interessato, ma anche nei confronti di chi acquista e utilizza tali sistemi[398]: più nel dettaglio, è necessario fornire tutta la documentazione tecnica che dimostri la *compliance* ai requisiti dettati dal regolamento (art. 11)[399]. *Ex* art. 13, i sistemi di intelligenza artificiale "ad alto rischio" devono essere progettati e sviluppati in modo da garantire che il loro funzionamento sia sufficientemente "*transparent*" e consentire agli utenti di interpretare agevolmente il funzionamento del modello algoritmico alla base del sistema[400]. Ne consegue l'obbligo di dotare i sistemi commercializzati di istruzioni per l'uso in un formato digitale appropriato, con informazioni «*concise, complete, correct and clear (…) relevant, accessible and comprehensible to users*»[401].

---

[396] Peraltro, è previsto che in una situazione di urgenza debitamente provata, l'uso del sistema possa avvenire anche senza autorizzazione, potendo essere convalidato durante o immediatamente dopo l'uso. EUROPEAN COMMISSION, *Proposal for a Regulation*, cit., art. 5, lett. *d*), pt. 3.

[397] I quali devono essere "*objective*" e "*clear*". Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation*, cit., art. 5, lett. *d*), pt. 3.

[398] Il tema sarà approfondito meglio *infra*, al § successivo.

[399] L'articolo 12 approfondisce il tema, stabilendo che «*high-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events ('logs') while the high-risk AI systems is operating. Those logging capabilities shall conform to recognised standards or common specifications. The logging capabilities shall ensure a level of traceability of the AI system's functioning throughout its lifecycle that is appropriate to the intended purpose of the system. In particular, logging capabilities shall enable the monitoring of the operation of the high-risk AI system with respect to the occurrence of situations that may result in the AI system presenting a risk within the meaning of Article 65(1) or lead to a substantial modification, and facilitate the post-market monitoring referred to in Article 61. For high-risk AI systems referred to in paragraph 1, point (a) of Annex III, the logging capabilities shall provide, at a minimum: (a) recording of the period of each use of the system (start date and time and end date and time of each use); (b) the reference database against which input data has been checked by the system; (c) the input data for which the search has led to a match; EN 50 EN (d) the identification of the natural persons involved in the verification of the results, as referred to in Article 14 (5)*».

[400] Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation,* cit., art. 13. Come si vedrà meglio *infra* al § 1.2, la necessità di garantire la trasparenza del processo decisionale algoritmico è stata di recente sottolineata anche nella Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, adottata dalla CEPEJ nel corso della sua 31ª Riunione plenaria (Strasburgo, 3-4 dicembre 2018).

[401] In particolare, le informazioni di cui al § 2 specificano: «*(a) the identity and the contact details of the provider and, where applicable, of its authorised representative; (b) the characteristics, capabilities and limitations of performance of the high-risk AI*

L'articolo 15 prescrive poi che i sistemi di intelligenza artificiale debbano essere progettati e sviluppati in modo da garantire l'accuratezza, la robustezza e la sicurezza del loro funzionamento. A tal proposito, è possibile scorgere nuovamente un'assonanza con quanto previsto dall'art. 32 GDPR, il quale richiede al titolare e al responsabile del trattamento dei dati di predisporre determinate misure tecniche e organizzative idonee per garantire un livello di sicurezza adeguato al rischio, tenendo conto dei potenziali pericoli presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata, o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. Peraltro, anche l'adeguatezza stessa delle misure tecniche di sicurezza dovrà essere costantemente monitorata, al fine di verificare se siano presenti determinate anomalie o irregolarità nel funzionamento dei sistemi.

Ulteriore elemento indispensabile per l'impiego di strumenti di IA ad "alto rischio" è rappresentato dalla previsione di una costante supervisione da parte di una persona fisica durante il periodo di utilizzo del sistema (art. 14, § 1). La disposizione si ritiene fondamentale, in quanto la Commissione europea sembra aver voluto ribadire formalmente quanto già da tempo avviene nella prassi per la maggior parte[402] dei sistemi automatici di identificazione biometrica[403] (ma non per tutti), ossia l'obbligatorietà di una convalida del risultato scaturito dal sistema di IA da parte di un operatore esperto. Infatti, tale supervisione e attività di controllo postumo da parte di un consulente tecnico, mira a prevenire o a ridurre al minimo i rischi per la salute, la sicurezza e i diritti fondamentali[404].

La proposta di regolamento costituisce certamente un punto di partenza adeguato per la regolamentazione delle tecniche di intelligenza artificiale. In tal senso, l'approccio basato sul rischio costituisce un primo efficace criterio di valutazione per numerose applicazioni che oggi rappresentano una potenziale minaccia per i diritti fondamentali. Allo stesso tempo, però, vien da chiedersi, come

system, including: (i) its intended purpose; (ii) the level of accuracy, robustness and cybersecurity referred to in Article 15 against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity; (iii) any known or foreseeable circumstance, related to the use of the highrisk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights; (iv) its performance as regards the persons or groups of persons on which the system is intended to be used; (v) when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the AI system. (c) the changes to the high-risk AI system and its performance which have been predetermined by the provider at the moment of the initial conformity assessment, if any; (d) the human oversight measures referred to in Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the users; (e) the expected lifetime of the high-risk AI system and any necessary maintenance and care measures to ensure the proper functioning of that AI system, including as regards software updates».

[402] Cfr. il capitolo I, § 3.5.1.

[403] Cfr. il capitolo I, §§ 3.1, 3.2, 3.3 e 3.6.

[404] Peraltro, come si vedrà meglio *infra* nel capitolo III, nonostante la ribadita importanza di una costante supervisione da parte di un operatore esperto nei confronti del sistema di IA, ciò che continua ad essere ancora un autentico arcano per i giudici è la valutazione delle conclusioni degli esperti. A tal proposito, J. Nieva-Fenoll, *Intelligenza artificiale e processo*, cit., p. 83, afferma che «è scioccante pensare che l'esperto di una specifica materia – il giurista – debba valutare le conclusioni di un esperto di un'altra materia che non conosce».

s'intende ulteriormente approfondire *infra*, se la regolamentazione dei sistemi d'identificazione biometrici sia sufficientemente efficace e circoscritta. Si ritiene che la futura normativa degli strumenti di identificazione biometrica non lesiva dei diritti fondamentali, seppur elastica e "adattabile" agli sviluppi delle tecniche di IA[405], dovrà essere più rigorosa e caratterizzata da limiti e facoltà più precisi[406].

2.2 I principi fondamentali in materia di intelligenza artificiale e giustizia alla luce del quadro giuridico attuale

Alla luce della ricostruzione normativa poc'anzi delineata, subentra una simultanea consapevolezza, come visto non sempre pienamente adeguata, in tutti gli attori coinvolti sulla scena della giustizia riguardo alle sfide lanciate dalla rivoluzione digitale e al ruolo essenziale che i diritti fondamentali assumono come sfondo imprescindibile per l'incontro tra i due mondi, delle scienze dure e delle scienze sociali. Risulta ragionevole a questo punto passare in rassegna i principi fondamentali che un sistema di IA deve rispettare per dirsi *compliant* tenuto conto del quadro giuridico appena descritto (cfr. §§ 2.1 e 2.1.1). In questo senso, gli atti che si prenderanno in considerazione, data la loro particolare pertinenza al tema, sono le *Ethics Guidelines for trustworthy AI* del gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale istituito dalla Commissione europea nel giugno 2018[407], la *Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia*

[405] Cfr. quanto affermato con riferimento alla nozione di "prova digitale" *supra*, al § 1.

[406] Sembra essere dello stesso avviso anche il Consiglio dell'Unione europea che ha di recente diffuso un primo testo di modifica delle disposizioni contenute nella proposta di regolamento della Commissione europea (COUNCIL OF THE EUROPEAN UNION, *Presidency compromise text*, 2021/0106(COD), 29.11.2021, reperibile all'indirizzo https://media-exp1.licdn.com/dms/document/C4D1FAQGuV1FL6qMDIA/feedshare-document-pdf-analyzed, (visualizzato in data 13.12.2021). Gli Stati membri ribadiscono la propria competenza esclusiva in materia di sicurezza nazionale e insistono sul fatto che i sistemi di intelligenza artificiale sviluppati esclusivamente per scopi militari dovrebbero essere esclusi dal campo di applicazione del regolamento. Altresì devono essere esclusi i sistemi di IA sviluppati al solo scopo di ricerca e sviluppo scientifici. Per quel che concerne i sistemi di riconoscimento biometrico, scompare dalla definizione l'aggettivo "remoti" per includere qualsiasi «*AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database data repository, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used*» (cfr. il considerando n. 8). Rispetto all'impiego da parte delle autorità di polizia di sistemi di riconoscimento "in tempo reale" in spazi accessibili al pubblico, è stato aggiunto all'articolo 5, par. 1, lett. *d*), che tali sistemi potrebbero essere utilizzati anche da altri soggetti che agiscono per conto delle autorità di contrasto o collaborano con esse. Al fine di garantire che tali sistemi siano utilizzati in modo responsabile e proporzionato, il Consiglio ha proposto che ognuna delle tre eccezioni sia descritta in modo più esaustivo e restrittivo, tenendo conto di alcuni elementi come, per esempio, la natura della situazione che ha dato origine alla richiesta, le conseguenze dell'uso per i diritti e le libertà di tutte le persone interessate e le garanzie e le condizioni previste per il suo utilizzo. Infine, dalla definizione di "*biometric data*" dell'articolo 3 (33) viene eliminata l'espressione «*which allow or confirm the unique identification of that natural person*». Ciò sembra essere un effettivo passo avanti nella costruzione di un glossario comune maggiormente rispondente alla realtà tecnico-forense (cfr. il capitolo I, § 1).

[407] Cfr. *supra* il § 2.1, il documento è reperibile all'indirizzo https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (visualizzato in data 22.4.2021).

(da qui in avanti *Carta etica*) emanata nell'ambito del Consiglio d'Europa nel dicembre 2018[408] e la nuova *proposta di Regolamento per un approccio europeo per l'intelligenza artificiale* della Commissione europea del 21 aprile 2021[409].

Si ritiene che la prima pietra angolare del quadro teorico-giuridico di riferimento sia rappresentata dal principio di "trasparenza"[410], ossia la possibilità di conoscere i dettagli tecnici che regolano il percorso seguito dal software per l'adozione della decisione automatizzata[411]. La necessità di accesso al funzionamento di un sistema di IA costituisce un incandescente crocevia di diverse opinioni nel dibattito sull'uso degli algoritmi nei processi decisionali, nel contesto sia pubblico che privato[412]. In particolare, le caratteristiche strutturali dei sistemi di IA parrebbero impedire o quantomeno rendere più complesso il soddisfacimento del requisito di trasparenza richiesto nel quadro giuridico europeo. Come già accennato *supra*, infatti, i *tools* di IA possono basarsi - *inter alia* - su meccanismi di apprendimento automatico (*machine learning* o *deep learning techniques*)[413], che consentono al

[408] Cfr. sempre il § 2.1, CEPEJ - *European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment*, reperibile su https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment (visualizzato in data 22.4.2021).

[409] Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation on a European approach for Artificial Intelligence*, COM(2021) 206 final, reperibile su https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence (visualizzato in data 23.4.2021).

[410] Il tema dell'accesso alle modalità di funzionamento di un determinato algoritmo ha già fatto il suo debutto in Italia nell'ambito della giurisprudenza amministrativa (cfr. Cons. Stato, 8.4.2019, n. 2270, reperibile su www.giustizia-amministrativa.it). Il supremo Consesso ha fissato alcuni principi che rendono legittimo il provvedimento integralmente automatizzato, tra i quali quello della conoscibilità del meccanismo che presiede alla decisione automatizzata «secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico» e che si estende agli autori, al procedimento utilizzato per la sua elaborazione, al meccanismo decisionale, comprensivo della procedura valutativa e decisionale dei dati selezionati come rilevanti, e quello dell'assoggettamento alla piena cognizione del giudice amministrativo, il quale deve essere posto in grado di poter sindacare la logicità e la ragionevolezza della regola che governa l'algoritmo. In precedenza, il TAR Lazio, sez. III-*bis*, 10.9.2018, n. 9227 ha affermato che «alcuna complicatezza o ampiezza, in termini di numero di soggetti coinvolti ed ambiti territoriali interessati, di una procedura amministrativa, può legittimare la sua devoluzione ad un meccanismo informatico o matematico del tutto impersonale e orfano di capacità valutazionali delle singole fattispecie concrete, tipiche invece della tradizionale e garantistica istruttoria procedimentale che deve informare l'attività amministrativa, specie ove sfociante in atti provvedimentali incisivi di posizioni giuridiche soggettive di soggetti privati e di conseguenziali ovvie ricadute anche sugli apparati e gli assetti della pubblica amministrazione». Per un commento sulla decisione, v. M. Catanzariti, *Enhancing Policing through Algorithmic Surveillance*, cit., p. 253.

[411] Cfr. M. Ebers, *Regulating AI and Robotics: Ethical and Legal Challenges*, in AA.VV., *Algorithms and Law*, (a cura di) M. Ebers, S. N. Navarro, Cambridge, Cambridge, University Press, 2019, p. 12 «*we can see only input data and output data for algorithm-based systems without understanding exactly what happens in between*», J. A. Kroll, J. Huey, S. Barocas, E. W. Felten, J. R. Reidenberg, D. G. Robinson & Harlan Yu, *Accountable Algorithms*, 165 *U. Pa. L. Rev.* 633 (2017), A. M. Crawford, 2018, *Seeing without knowing: limitations of the transparency ideal and its application to algorithmic accountability* in *New Media Soc*, 20:973, P. Perri, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè, Milano, 2020, p. 134, F. Palmiotto, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in AA.VV., *Algorithmic Governance and Governance of Algorithms, Legal and Ethical Challenges*, (a cura di) M. Ebers, M. Cantero Gamito, Springer, 2020, pp. 56 e ss. e F. Palmiotto, *The Right to Contest Automated Decisions*, 14.2.2022, reperibile all'indirizzo https://digi-con.org/the-right-to-contest-automated-decisions/ (visualizzato in data 21.2.2022).

[412] Cfr. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, p. 17 e G. Ziccardi, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina ed., Milano, 2015, pp. 11 e ss.

[413] Cfr. *supra* il § 2.

sistema di imparare in modo autonomo a compiere una determinata operazione anche se questa non era stata programmata tra le possibili scelte. Tali sistemi, denominati anche "scatole nere" o "*black box*", risultano difficilmente intellegibili dagli operatori, rendendo praticamente impossibile l'operazione di ottenimento delle informazioni sui criteri in base ai quali opera l'algoritmo[414]. Peraltro, per superare questo problema, c'è chi ha osservato che il meccanismo di funzionamento di una "*black box*" potrebbe essere accostato anche al funzionamento della mente umana, le cui decisioni sono adottate sulla base di emozioni o impulsi comunque senza seguire una logica riconoscibile[415]. Secondo tale indirizzo interpretativo, le decisioni giudiziali sarebbero influenzate non raramente «dalle sensazioni, dai sentimenti, dalle intuizioni»[416], ma si ritiene comunque che ciò non possa in alcun modo giustificare l'ammissibilità di scelte algoritmiche che incidono nella sfera giuridica di un soggetto senza che questi possa verificare la correttezza del procedimento informatico. In tal senso, con riferimento alle esigenze di tutela della proprietà intellettuale, deve prevalere l'accessibilità al processo algoritmico. Tale valore può essere assicurato attraverso una completa trasparenza tecnica (del codice sorgente e della documentazione), non sempre di per sé però sufficiente. È stato correttamente evidenziato che, anche se sia possibile compiere il cd. *reverse engeneering*, la comprensione del modello potrebbe rimanere una questione limitata alla conoscenza degli esperti, con l'esclusione dei destinatari effettivi[417]. Nel processo penale non possono esserci scatole nere in cui non solo i giuristi, ma anche i cittadini in generale non possono entrare e informarsi, dal momento che, come si approfondirà meglio *infra*[418], questo sarebbe lesivo della garanzia fondamentale del diritto di difesa e di pubblicità della decisione. In tal senso, la trasparenza degli algoritmi è stata elevata a rango di nuova e ulteriore garanzia del sistema a partire già dal GDPR che, in diverse parti[419], richiama il requisito con riferimento alle modalità di trattamento con cui sono «raccolti, utilizzati, consultati o altrimenti trattati dati personali […] nonché la misura in cui i dati personali sono o saranno trattati»[420]. In questo contesto, il principio di trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Ne consegue una logica applicazione anche a

[414] Cfr. F. Donati, *Intelligenza artificiale e giustizia*, cit., p. 427.
[415] Per un approfondimento sul tema cfr. J. A. Seaman, *Black Boxes*, in *Emory Law Journal* 58, no. 2 (2008): pp. 427-488.
[416] Cfr. G. Legnini, *Introduzione*, in AA.VV., *Decisione robotica*, (a cura di) A. Carleo, Il Mulino, Bologna, 2019, p. 12.
[417] Cfr. su questo specifico punto S. Quattrocolo, *Intelligenza artificiale e giustizia nella cornice della Carta etica europea. Gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *www.lalegislazionepenale.it*, 2018.
[418] Cfr. il capitolo III, § 2.2.
[419] Cfr. i considerandi nn. 39, 58, 60, 71, 78, 100 e 121, e il requisito viene menzionato agli artt. 5, 12, 13, 53 e 88.
[420] Cfr. il considerando n. 39, GDPR, cit.

scenari dominati da strumenti che si servono di tecniche di intelligenza artificiale, interessati da un sistematico utilizzo di dati personali[421].

Volendo utilizzare un criterio cronologico, nel dicembre 2018, come visto *supra*[422], è stata introdotta la *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*[423]. Nel documento di *soft law* viene ribadito il rispetto del principio in esame, ponendolo in stretto collegamento con l'imparzialità e *fairness* (art. 4): in particolare la Carta raccomanda l'accessibilità, la comprensibilità e la verificabilità esterna dei processi computazionali utilizzati per l'analisi dei dati giudiziari. Con riferimento a tale prescrizione, è possibile intuire tra le righe una preoccupazione della CEPEJ di cui si è già fatto cenno poc'anzi[424], ossia la complessità del rapporto tra la protezione della proprietà intellettuale e del *trade secret* e la necessità di osservare, capire e verificare i processi computazionali utilizzati. In tal senso, si ribadisce che l'interesse della giustizia debba sempre prevalere nel bilanciamento con gli interessi privati di chi ha creato effettivamente il *software*. Così, la Carta ha auspicato un regime di completa "trasparenza tecnica", accompagnata dalla cd. "spiegabilità" del processo computazionale in un linguaggio accessibile e chiaro[425]. Mentre la prima implica la possibilità di avere accesso a tutti gli aspetti tecnici del software in uso, compresi i cd. codici sorgente, la seconda consiste in una descrizione del procedimento mediante il quale un decisore, considerando un insieme di dati di *input*, ha raggiunto una determinata conclusione[426]. Entro il contesto della giustizia penale, questo assume un significato ancora più di rilievo, legato al principio di pubblicità del processo decisionale e, più in particolare, al momento della valutazione della prova. Rispetto a questo, si è già evidenziato come la trasparenza algoritmica non sia di per sé un obiettivo sufficiente per fornire ai reali destinatari informazioni comprensibili sulla decisione. Un'opzione possibile, delineata dalla Carta, allora, sta nella creazione di autorità indipendenti che possano di volta in volta verificare e certificare aprioristicamente e periodicamente gli algoritmi utilizzati nei servizi di giustizia. Trattasi di una soluzione ispirata proprio a imparzialità e *fairness*[427].

---

[421] In tal senso nel considerando n. 39, GDPR, cit. si afferma che «*that principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed*».

[422] Cfr. il § 2.1.

[423] Cfr. https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348 (visualizzato in data 29.4.2021).

[424] Cfr. il § 2.2.

[425] Cfr. S. Quattrocolo, *Intelligenza artificiale e giustizia nella cornice della Carta etica europea. Gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *www.lalegislazionepenale.it*, 2018.

[426] Trattasi di due principi distinti ma strettamente correlati. Cfr. F. Palmiotto, *The Right to Contest Automated Decisions*, 14.2.2022, cit.

[427] Cfr. S. Quattrocolo, *Intelligenza artificiale e giustizia nella cornice della Carta etica europea*, cit.

Con le *Ethics Guidelines for trustworthy AI* del 2019 è stato successivamente ribadito il principio di trasparenza algoritmica nei seguenti termini[428]. Le linee guida evidenziano in particolare che i *set* dei dati e i processi algoritmici che determinano la decisione del sistema di IA dovrebbero essere sempre documentati secondo i migliori standard esistenti al fine di consentire la tracciabilità e la trasparenza. Oltre a ciò, è previsto che anche il metodo di apprendimento del sistema di IA sia pedissequamente documentato e che possa essere data adeguata verifica alla raccolta e alla selezione dei dati. In altre parole, la tracciabilità facilita la verificabilità e la spiegabilità del sistema algoritmico. A tal proposito, il documento definisce tale ultimo tratto come la capacità di spiegare sia i processi tecnici di un sistema di IA, sia le relative decisioni umane. Il principio assume rilevanza nella misura in cui se un sistema di IA influisce considerevolmente sulla vita delle persone, dovrebbe essere sempre consentito richiedere una spiegazione del processo decisionale del sistema: quest'ultima dovrebbe essere tempestiva e sempre adeguata alle competenze del destinatario direttamente interessato.

Come già accennato poc'anzi[429], anche la recente proposta di regolamento - *Artificial Intelligence Act* - conferma il necessario rispetto del requisito in parola[430]. A tal proposito, sono previsti diversi livelli di *transparency*: a seconda del livello di "rischio" associato all'utilizzo di un determinato strumento di IA è prevista una corrispondente proporzione in termini di trasparenza algoritmica. Quindi, per alcuni specifici sistemi "a basso rischio" sono proposti obblighi minimi di trasparenza[431], per gli strumenti considerati ad "alto rischio"[432], invece, il rispetto del requisito risulta strettamente

[428] Cfr. *Ethics guidelines for trustworthy AI*, p. 18, reperibili all'indirizzo https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (visualizzato in data 29.4.2021).

[429] Cfr. *supra* il § 2.1

[430] Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation*, cit., art. 13.

[431] Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation*, cit., p. 3.

[432] Si rammenta che i sistemi ad alto rischio sono specificati nell'appendice alla proposta di regolamento. In particolare, tra essi sono annoverati «*1. Biometric identification and categorisation of natural persons: (a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons; 2. Management and operation of critical infrastructure: (a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity. 3. Education and vocational training: (a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions; (b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions. 4. Employment, workers management and access to self-employment: (a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests; (b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships. 5. Access to and enjoyment of essential private services and public services and benefits: (a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services; (b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use; (c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid. 6. Law enforcement: (a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences; (b) AI systems intended to be used by law enforcement authorities as polygraphs and similar*

necessario al fine quantomeno di «*mitigate the risks to fundamental rights*»[433]. In particolare, l'articolo 13 della proposta di regolamento stabilisce che i sistemi di IA ad alto rischio devono essere progettati e sviluppati in modo da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l'*output* del sistema e utilizzarlo in modo appropriato[434]. Si prevede che tali strumenti di IA siano accompagnati da istruzioni concernenti il loro utilizzo e una serie di informazioni quali l'identità e i recapiti del fornitore, la destinazione d'impiego del *tool*, il livello di accuratezza, robustezza e sicurezza informatica[435]. Come visto[436], quest'ultimo aspetto è disciplinato più specificamente all'art. 15, ove viene stabilito che i sistemi di IA devono garantire un adeguato livello di precisione rispetto alla destinazione d'impiego[437]. Accuratezza, robustezza e sicurezza sono tratti che non suonano del tutto inediti in quanto già in precedenza, con la Carta etica,

tools or to detect the emotional state of a natural person; (c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3); (d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences; (e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups; (f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences; (g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data. 7. Migration, asylum and border control management: (a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person; (b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State; (c) AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features; (d) AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status. 8. Administration of justice and democratic processes: (a) AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts». Cfr. ANNEXES to the *Proposal for a Regulation of the European Parliament and of the Council Laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts* reperibile all'indirizzo https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence (visualizzato il 29.4.2021).

[433] Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation*, cit., p. 7.

[434] Il Parlamento europeo, tramite il COMMITTEE ON LEGAL AFFAIRS FOR THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION AND THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft Opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts* (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 2.3.2022, ha specificato ulteriormente che «(…) *transparency shall thereby mean that, to the extent that can be reasonably expected and is feasible in technical terms at the time when the AI system is placed on the market, the AI system is interpretable to the provider, in that the provider can understand the rationale of decisions taken by the high risk AI system, while enabling the user to understand and use the AI system appropriately, by generally knowing how the AI system works and what data it ingests*» (Art. 13, par. 1).

[435] Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation*, cit., art. 13, §§ 2 e 3 e F. Palmiotto, *The Right to Contest Automated Decisions*, 14.2.2022, cit.

[436] Cfr. il § 2.1.

[437] Di particolare interesse è il § 4, il quale considerando tali strumenti stabilisce la necessaria attribuibilità di un carattere di "resilienza" rispetto ai tentativi da parte di soggetti terzi non autorizzati di modificare il loro uso e le loro prestazioni sfruttando le vulnerabilità del sistema.

era stato sancito all'art. 3 il principio di qualità e sicurezza: da una parte, si raccomanda di utilizzare esclusivamente dati provenienti da fonti certificate, dall'altra il procedimento deve essere tracciabile e i modelli e gli algoritmi creati dovevano poter essere memorizzati ed eseguiti in ambienti sicuri, in modo da garantire l'integrità del sistema[438].

Dalla carrellata di atti normativi richiamati risulta però evidente come una tecnologia di intelligenza artificiale trasparente e spiegabile costituisca, da qualche tempo, una sfida che impegna tutte le autorità nazionali e soprattutto sovranazionali, con l'obiettivo di arginare l'ormai tipica aura di opacità algoritmica[439]. In una società dominata da un continuo scambio di dati digitali, il rischio che si corre è quello di deprivare completamente i soggetti processuali, e in primo luogo le parti, della loro rilevanza all'interno dell'*iter* probatorio (dalla fase di raccolta alla valutazione). Nell'attuale panorama normativo europeo, non solo processuale, è possibile cogliere così adeguate reazioni ai predetti pericoli: a tal proposito giova ricordare il movimento scientifico volto a sviluppare una "*Explainable Artificial Intelligence*" (XAI)[440], il quale individua una serie di requisiti cui deve rispondere un algoritmo per poter essere qualificato come "*explainable*"[441].

Sebbene non sia stata ancora direttamente esplicitata e definita da un punto di vista normativo[442], strettamente connessa al principio di trasparenza è l'*interpretabilità*[443]. L'effettiva trasparenza di un

---

[438] Giova ricordare che il Parlamento europeo, tramite il COMMITTEE ON LEGAL AFFAIRS FOR THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION AND THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft Opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, cit., p. 34 ha proposto di emedare l'art. 4 della proposta di regolamento della Commissione europea, specificando ulteriormente che «*providers of an AI system shall, throughout all stages of development of the AI system, acknowledge the EU Charta of Fundamental Rights and ensure that the AI system is lawful, ethical and robust. (a) 'lawful' means that the AIsystem is developed to operate in accordance with European, national and international legally binding rules; (b) 'ethical' means that the AI system is developed taking into account the specific benefits of the AI system while respecting the freedom and autonomy of human beings, human dignity as well as mental and physical integrity, and to be fair and explicable; (c) 'robust' means that the AI system performs in a safe, secure and reliable manner, with embedded safeguards to as much as possible prevent any unintended adverse impacts*».

[439] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., pp 210 e ss. e F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harward University Press, Cambridge-London, 2015.

[440] Per un approfondimento sul punto v. https://www.darpa.mil/program/explainable-artificial-intelligence (visualizzato in data 24.5.2021).

[441] Cfr. sul punto B. Waltl, R. Vogl, *Explainable Artificial Intelligence – the New Frontier in Legal Informatics*, in *Jusletter* IT, 22.2.2018.

[442] Anche in letteratura si registra una certa sovrapposizione concettuale tra le espressioni "*transparency*", "*explainability*" e "*interpretability*". Cfr. F. Palmiotto, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in AA.VV., *Algorithmic Governance and Governance of Algorithms, Legal and Ethical Challenges*, (a cura di) M. Ebers, M. Cantero Gamito, Springer, 2020, pp. 56 e ss. Oltre a ciò, bisogna tenere in considerazione che la *explainability* o *interpretability* di un sistema di IA dipende da diversi fattori: il grado di conoscenza tecnologica che un soggetto ha; le finalità di questa conoscenza; il linguaggio con cui si richiedono spiegazioni; se la spiegazione debba essere richiesta per una sola decisione o per tutto il sistema di IA. Cfr. anche G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., pp. 212 e ss.

[443] La nozione di "interpretabilità" non è stata ancora univocamente definita in letteratura. Su questo punto, cfr. Z.C., Lipton, *The mythos of model interpretability*, in *arXiv*, 2016 e A.K. Jain, D. Deb, J.J. Engelsma, *Biometrics: Trust, but Verify*, in *https://arxiv.org/abs/2105.06625*, 14.5.2021, p. 9.

sistema algoritmico dipende dalla precisione della teoria scientifica che la sostiene e, in secondo luogo, dalla chiarezza del linguaggio utilizzato per tradurlo in un sistema matematico[444]. Da un punto di vista informatico, infatti, un linguaggio matematico chiaro permette ad un operatore di comprendere *ex post* il procedimento che da un dato *input* ha portato ad un determinato *output*[445]. Da qui, parte della letteratura specializzata in questo ambito la definisce come «*the degree to which a human can understand the cause of a decision*»[446], altra parte invece come «*the degree to which a human can consistently predict the model's result*»[447]. L'obiettivo delle più recenti ricerche sul campo è rappresentato dalla creazione di una serie di metodi interpretabili che producano "modelli" di funzionamento degli algoritmi più spiegabili, conservando al contempo elevati livelli di prestazione. Nell'ultimo decennio, infatti, il ritmo dei progressi verso la risoluzione di tali problematiche è rallentato drasticamente, dal momento che la ricerca sull'IA si è concentrata prioritariamente verso lo sviluppo di algoritmi dotati di un'elevata capacità predittiva, mentre la comprensione dei processi decisionali ha assunto una posizione di subordine in termini di importanza. In realtà, si ritiene che, affinché un sistema di IA possa dirsi affidabile, occorre comprendere perché si è comportato in un certo modo. In questo senso, l'" interpretabilità" si pone come un requisito *trait d'union* fra la "trasparenza" e la "spiegabilità", richiedendo che un sistema di IA possa definirsi come una *white box*, o cd. "scatola di vetro", attraverso l'analisi del modello logico di apprendimento alla base del sistema considerato. La spiegabilità in questo senso si riferisce ad una più ampia serie di considerazioni che rendono un sistema di intelligenza artificiale altamente comprensibile ai destinatari, tra cui la descrizione del procedimento che rende tutte le informazioni del sistema di IA direttamente accessibili agli utenti. Tra IA spiegabile e IA interpretabile la finalità rimane la stessa, ossia la trasparenza "rafforzata" dell'algoritmo posto alla base del funzionamento di un sistema[448]. A questo scopo, pertanto, è necessario tenere a mente tutte le differenti declinazioni del principio descritto non solo al momento della progettazione, ma anche per il successivo sviluppo e utilizzo dello strumento di IA.

Ulteriore principio etico più o meno valorizzato all'interno dei tre documenti è la *fairness*. Con le *Ethics Guidelines for trustworthy AI*, il principio di equità è stato inteso in senso sia sostanziale sia processuale. Il primo implica un impegno a garantire una distribuzione giusta ed equa di costi e di benefici e ad assicurare che gli individui e i gruppi siano liberi da distorsioni inique, discriminazioni

[444] Cfr. C. Villani, *AI for Humanity—French National Strategy for Artificial intelligence*, 2018, reperibile all'indirizzo https://www.aiforhumanity.fr/en/ (visualizzato il 29.4.2021) e A.K. Jain, D. Deb, J.J. Engelsma, *Biometrics: Trust, but Verify*, cit., p. 10.

[445] Cfr. V. Carvalho, E. M. Pereira, J. S. Cardoso, *Machine Learning Interpretability: A Survey on Methods and Metrics*, in *Electronics*, 2019, 8, p. 832.

[446] Cfr. T. Miller, *Explanation in Artificial Intelligence: Insights from the social sciences*, in *Artif. Intell*., 2018, 267, pp. 1 e ss.

[447] Cfr. B. Kim, R. Khanna, O.O. Koyejo, *Examples are not enough, learn to criticize! Criticism for interpretability*, in *Advances in Neural Information Processing Systems*, MIT Press, Cambridge, 2016, pp. 2280 e ss.

[448] Fornisce una spiegazione su come l'algoritmo crea il modello.

e stigmatizzazioni. In questo modo, riuscendo ad evitare tali alterazioni, i sistemi di IA potrebbero persino aumentare l'equità sociale. La dimensione procedurale dell'equità implica invece la capacità di impugnare le decisioni elaborate dai sistemi di IA e dagli esseri umani. In coerenza con ciò, l'organismo responsabile della decisione deve essere identificabile e i processi decisionali devono essere spiegabili. L'equità risulta quindi strettamente connessa ai principi di non discriminazione, di solidarietà e di giustizia (artt. 21 e ss.).

Con la *Carta etica europea*, si ribadisce con enfasi uno stretto collegamento logico tra *fairness* e *imparzialità* e *trasparenza*: in particolare, si raccomanda l'accessibilità, la comprensibilità e la verificabilità esterna dei processi computazionali utilizzati per l'analisi dei dati giudiziari. Come già poc'anzi accennato, nel bilanciamento fra l'interesse di assicurare la giustizia e quello privato dello sviluppatore del software deve prevalere il primo e questo può avvenire solo se tutto il ciclo di progettazione, sviluppo e utilizzo del modello è ispirato ai tre requisiti richiamati. Il documento su questo punto non si espone ulteriormente, lasciando alle autorità dei diversi Stati membri la possibilità di cogliere e modellare il suggerimento in base alle caratteristiche di ciascun ordinamento[449].

Infine, nella nuova proposta di regolamento della Commissione europea scompare il riferimento alla *fairness* in corrispondenza diretta della disciplina in materia di *transparency*, quasi volendo dare per scontato quanto già fermamente statuito, a distanza di pochi mesi tra loro, dalle *Guidelines* e dalla *Carta etica europea*[450]. Tuttavia, di *fairness* si fa cenno con riferimento al *trial*: come è ormai noto, l'uso dell'IA con le sue peculiari caratteristiche può incidere negativamente su una serie di diritti e garanzie sanciti dalla Carta dei diritti fondamentali dell'UE. Attraverso un approccio basato sul rischio e un elenco di requisiti obbligatori da rispettare, proporzionati per tutti i partecipanti al ciclo del modello algoritmico, la proposta mira proprio a garantire e rafforzare tali diritti, tra i quali quello ad un processo equo[451].

In tutti e tre i documenti, poi, si fa cenno al generale rispetto dei diritti fondamentali (*lawfulness*), assicurando che l'elaborazione e l'utilizzo di strumenti e servizi di intelligenza artificiale siano compatibili con i diritti fondamentali. Tale principio si rivolge non solo e principalmente agli Stati, ma per lo più a singoli individui e, in particolare, a operatori del settore direttamente coinvolti nella progettazione dei software. Più nel dettaglio, nella nota esplicativa della Carta etica si evidenzia come tali strumenti di IA debbano essere progettati seguendo un approccio *human-rights-by-design*, ossia

[449] Cfr. S. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea*, cit.

[450] Il principio è stato brevemente richiamato anche dalla *European Parliament resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice* (2020/2013(INI)) – https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html, peraltro generalmente attribuito, come principio "guida", con riferimento ai sistemi di intelligenza artificiale, senza ulteriori specificazioni.

[451] Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation*, cit., p. 11 e ribadito negli stessi termini al considerando n. 28.

in un'ottica di protezione dai potenziali rischi di violazione dei diritti fondamentali che, nel più circoscritto ambito dell'amministrazione della giustizia, attengono - a titolo esemplificativo e non esaustivo - al diritto di accesso alla giurisdizione, al diritto ad un processo equo, alla parità delle armi, al principio di legalità, alla libertà personale/morale etc.[452]. Entro tale scenario viene ribadito più volte il principio di non discriminazione, ponendo specificamente il divieto in tutti gli atti finora esaminati, nell'utilizzo di strumenti di IA, di creare o accentuare forme di discriminazione tra gruppi e individui[453]. Nel suo impiego, infatti, l'idea che l'IA possa eliminare o addirittura ridurre gli errori o i pregiudizi che possono condizionare l'esito del procedimento è stata da tempo ritenuta infondata[454]. Gli errori e i pregiudizi già insiti nel pensiero umano possono riprodursi ed essere perfino amplificati dalle tecniche di IA[455], come è avvenuto per esempio nella nota vicenda in cui è stato applicato il sistema COMPAS[456], ossia un programma informatico avente la finalità di calcolare il rischio di recidiva e la pericolosità sociale delle persone[457]. Come noto, il rischio può verificarsi a più livelli[458]: l'*input* non risultando sempre completamente neutro potrebbe influenzare l'*output*, generando la discriminazione di singoli individui o di interi gruppi sociali[459]; secondariamente, la deriva discriminatoria potrebbe manifestarsi con la riproduzione di ingiustificati pregiudizi sociali[460]. Infine, la decisione sulla previsione di recidiva presa da un software in un momento precedente alla commissione di eventuali nuovi fatti di reato costituisce già di per sé il frutto di un procedimento logico-deduttivo evidentemente errato.

Pertanto, sia i soggetti pubblici sia i privati devono garantire che gli strumenti di IA non conducano ad analisi discriminatorie, a maggior ragione quando si considerino dati sensibili quali quelli relativi all'origine razziale o etnica, al *background* socio-economico, alle opinioni politiche, ai dati genetici o

---

[452] Cfr. S. Quattrocolo, *Intelligenza artificiale e giustizia nella cornice della Carta etica europea. Gli spunti per un'urgente discussione tra scienze penali e informatiche*, cit. Per un approfondimento sul *template* nello spettro delle garanzie processuali penali fondamentali, v. *infra* il capitolo III.

[453] Per un approfondimento sul concetto di "*bias*" e le possibili distorsioni della tecnologia automatica di riconoscimento facciale cfr. *infra* il capitolo IV, § 3.1.2.

[454] Cfr. F. Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Cambridge, London, 2015, pp. 102 e ss. e F. Donati, *Intelligenza artificiale e giustizia*, in *Rivista AIC*, 1/2020, 2.3.2020, p. 421.

[455] Cfr. M. Ebers, *Regulating AI and Robotics: Ethical and Legal Challenges*, in AA.VV., *Algorithms and Law*, (a cura di) M. Ebers, S. N. Navarro, Cambridge, University Press, 2019, p. 33.

[456] COMPAS è l'acronimo di *Correctional Offenders Management Profilying for Alternative Sanctions*. COMPAS è un software che valuta il rischio di recidiva per mezzo di un'analisi statistica basata su informazioni ottenute tramite i colloqui con l'imputato e sui dati giudiziari relativi allo stesso, valutati sulla base di dati statistici prendendo in considerazione un campione di popolazione. Il software è stato progettato da Northpointe inc. V. F. Donati, *Intelligenza artificiale e giustizia*, cit., p. 421.

[457] Per un approfondimento sul punto cfr. S. Quattrocolo, *Equo processo e sfide della società algoritmica*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2019, pp. 135-144.

[458] Cfr. Appendice esplicativa alla Carta etica europea, reperibile all'indirizzo https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348 (visualizzato in data 30.4.2021).

[459] Cfr. S. Quattrocolo, *Intelligenza artificiale e giustizia nella cornice della Carta etica europea*, cit.

[460] Su questo punto la letteratura risulta assai ricca, v. *ex multis* T.P. Woods, *The Implicit Bias of the Implicit Bias Theory*, in *Drexel Law Review*, 2017, pp. 631 e ss.

biometrici. Qualora tale *output* discriminatorio venga individuato, occorre necessariamente disporre una misura correttiva al fine di limitare o, se possibile, neutralizzare questi rischi, sensibilizzando i destinatari della decisione algoritmica. Come ragionevolmente suggerito dalla dottrina, una soluzione a questi usi distorti di IA potrebbe essere rappresentata da un coordinamento scientifico fra, da una parte, esperti di intelligenza artificiale e *computer science* e, dall'altra, studiosi di processi e interazioni sociali, al fine di analizzare eventuali conseguenze patologiche scaturenti dal ricorso a *data set* non del tutto neutri[461].

Quanto al principio di qualità e di sicurezza, esso si trova sancito ancora una volta in tutti i documenti summenzionati. Mentre nelle *Ethics Guidelines for trustworthy AI* si separa il criterio disciplinando la "robustezza tecnica e sicurezza" del sistema e la "qualità e integrità" dei dati, la *Carta etica europea* considera i requisiti strettamente connessi e, quindi, con riferimento all'analisi dei dati e delle decisioni giudiziarie, li enuncia come principio unico. In particolare, il documento raccomanda l'utilizzo di fonti certificate e di dati intangibili, attraverso modelli concepiti in modo multidisciplinare, in un ambiente tecnologico sicuro. La prima parte della disposizione si concentra in modo specifico sulla sicurezza dei dati giudiziari trattati attraverso sistemi computazionali. Al fine di verificare potenziali modificazioni dei dati, accidentali o strumentali, l'intero procedimento deve essere tracciato e documentato[462]. Infine, la recente proposta di regolamento, come già visto *supra*[463], dedica un'intera disposizione (art. 15) al principio, sancendo che i sistemi di IA ad "alto rischio" debbano essere progettati e sviluppati in modo da raggiungere, alla luce della destinazione d'impiego, un livello adeguato di precisione, robustezza e sicurezza informatica. Tali classi di accuratezza sono dichiarate nelle istruzioni d'uso allegate al sistema di IA e, in aggiunta rispetto agli altri due documenti richiamati, si prescrive un requisito di "resilienza" con riferimento agli errori, guasti o incongruenze che possono verificarsi all'interno del sistema o dell'ambiente in cui si opera. Lo stesso parametro concerne anche i tentativi da parte di soggetti terzi non autorizzati di modificare l'utilizzo dello strumento o le loro prestazioni sfruttando le vulnerabilità del sistema (art. 15, § 4). A tal proposito, le soluzioni tecniche proposte per le vulnerabilità dei sistemi comprendono misure che prevengono la manipolazione dei dati di addestramento (cd. *data poisoning*) o un errore nel modello (cd. *adversarial examples*).

Quanto all'intervento e alla sorveglianza da parte di un operatore nello sviluppo e utilizzo di un sistema di IA, fra i requisiti fondamentali posti alla base di un *tool* affidabile, viene annoverata anche la doverosità di un controllo diretto da parte degli utenti. In tal senso, la sorveglianza umana aiuta a

[461] Cfr. S. Quattrocolo, *Intelligenza artificiale e giustizia nella cornice della Carta etica europea*, cit.
[462] Cfr. S. Quattrocolo, *Intelligenza artificiale e giustizia nella cornice della Carta etica europea*, cit
[463] Cfr. il § 2.1.

garantire che un sistema di IA non provochi potenziali effetti negativi. Tale forma di controllo può avvenire attraverso meccanismi di *governance* che ammettano un intervento umano (cd. *human in the loop* – HITL)[464], con supervisione umana (cd. *human on the loop* – HOTL)[465] o con controllo umano (cd. *human in command* –HIC)[466]. Le linee guida suggeriscono, poi, ulteriori diverse soluzioni che consentono sempre di garantire che il processo decisionale non sia gestito unicamente dal modello algoritmico: per esempio, una prima proposta è quella di non utilizzare un sistema di IA in una data situazione che non permette un intervento umano, ovvero quella di stabilire dei livelli di discrezionalità umana durante l'impiego del sistema, o, ancora, di garantire la capacità di ignorare una decisione presa univocamente dallo strumento automatico. Viene sancito il principio secondo cui a parità di condizioni, minore è la sorveglianza che un essere umano può esercitare su un sistema di IA, maggiore è la necessità di una *governance* rigorosa. Per tale ragione, le *guidelines* concludono affermando che potrebbe essere necessaria l'introduzione di alcuni meccanismi di sorveglianza a vari livelli, a sostegno di altre misure di sicurezza e di controllo, a seconda del settore di applicazione del sistema di IA e del potenziale rischio[467]. In una stretta connessione logica rispetto a quanto appena affermato risulta, poi, il concetto di *accountability*[468], per cui si prevede la nomina di un soggetto responsabile delle questioni etiche relative all'IA o di un *panel* etico che assolva lo specifico compito di prestare sorveglianza e fornire consulenza. Viene poi stilata una cd. "lista di controllo", principalmente destinata a sviluppatori e distributori di sistemi di IA al fine di rendere operativa un'IA affidabile che interagisca direttamente con gli utenti[469].

Il quinto principio sancito dalla *Carta etica europea* è rappresentato proprio dalla garanzia di cd. *under user control*, escludendo un approccio prescrittivo dell'impiego di intelligenza artificiale e garantendo che gli utilizzatori possano agire come soggetti informati, nel pieno controllo delle loro scelte. L'utente è individuabile sia nell'operatore del diritto che si serve del *tool*, sia nell'interessato destinatario della decisione, traducendosi per il primo nella possibilità di riesaminare le decisioni e i dati utilizzati per la produzione di un certo risultato, continuando a non essere vincolati a esso alla luce delle caratteristiche specifiche del caso concreto; per il secondo, invece, nell'utilizzo informato

[464] L'approccio HITL prevede la possibilità di intervento umano in ogni ciclo decisionale del sistema, che in molti casi non è né possibile né auspicabile. Cfr. *Ethics guidelines for trustworthy AI*, cit., p. 18

[465] L'approccio HOTL prevede l'intervento umano durante il ciclo di progettazione del sistema e il monitoraggio del funzionamento del sistema. Cfr. *Ethics guidelines for trustworthy AI*, cit., p. 18

[466] L'approccio HIC prevede il controllo dell'attività del sistema di IA nel suo complesso (compresi i suoi effetti generali a livello economico, sociale, giuridico ed etico) e la capacità di decidere quando e come utilizzare il sistema in qualsiasi particolare situazione. Cfr. *Ethics guidelines for trustworthy AI*, cit., p. 18

[467] Cfr. *Ethics guidelines for trustworthy AI*, cit., p. 18.

[468] Cfr. *Ethics guidelines for trustworthy AI*, cit., p. 26.

[469] Cfr. *Ethics guidelines for trustworthy AI*, cit., pp. 30 e ss.

del sistema di IA fornito di un linguaggio chiaro e comprensibile, del carattere vincolante o meno delle soluzioni proposte e del diritto a ricevere assistenza legale e l'accesso a un tribunale.

In generale, la Carta etica tiene a sottolineare che quando venga attuato un sistema informativo basato sull'IA dovrebbero essere sviluppati programmi di alfabetizzazione informatica, destinati agli utilizzatori, e dibattiti che includano anche la categoria dei professionisti della giustizia[470]. Pertanto, una delle più lampanti implicazioni sembra proprio essere l'introduzione di un'adeguata letteratura esplicativa e di un dibattito multidisciplinare che coinvolga anche i giuristi[471].

Infine, la recente proposta di regolamento dedica un'intera disposizione all'esercizio di un controllo da parte dell'utente (art. 14). In particolare, i sistemi di IA "ad alto rischio" devono essere progettati e sviluppati con la dotazione di adeguati strumenti di interfaccia uomo-macchina, al fine di garantire un efficace controllo da parte di persone fisiche, durante l'intero periodo di utilizzo del sistema. L'obiettivo principale è quello di prevenire o quantomeno ridurre al minimo, i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA sia utilizzato con modalità non conformi alla sua destinazione o in condizioni d'uso improprio. Al § 4 sono espressamente indicate le caratteristiche che tali misure di controllo devono garantire all'utente: la comprensione delle capacità e i limiti del sistema di IA, potendo monitorarne debitamente l'intero funzionamento (lett. *a*); la consapevolezza di un cd. *bias* di automazione[472], conseguente ad un uso distorto dei sistemi di IA; la possibilità di interpretare correttamente i risultati del sistema di IA, tenendo in considerazione le caratteristiche del *tool*; la possibilità di decidere in qualsiasi momento di non utilizzare più lo strumento di IA o di ignorare l'*output* dello stesso e essere in grado di intervenire sul funzionamento del sistema. Questi, unitamente agli obblighi dei fornitori (art. 16), degli importatori (art. 26), dei distributori (art. 27) e, infine, degli utenti stessi (art. 29) garantiscono l'esercizio di un controllo costante sugli strumenti di IA. Più nel dettaglio, tra gli obblighi per i fornitori è prevista, come nelle *Ethics guidelines*, la messa a punto di un quadro giuridico che definisca la responsabilità della direzione e del personale coinvolto nella progettazione e nello sviluppo del sistema di IA.

Giova infine fare cenno alla *reliability*. Con le *Ethics Guidelines for Trustworthy AI*, l'affidabilità costituisce un obiettivo più che un criterio da rispettare. Solo tendendo il più possibile verso un'IA *reliable* gli individui destinatari dei procedimenti algoritmici automatici potranno avere fiducia nello

[470] In tale contesto, l'*accountability* dei proprietari dei software viene solo brevemente citato come un dato da tenere in considerazione nell'utilizzo dei sistemi di IA, senza specificarne ulteriori aspetti correlati. Cfr. CEPEJ, *Appendix I – In-depth study on the use of AI in judicial systems, notably AI applications processing judicial decisions and data*, cit., p. 54.

[471] Cfr. S. Quattrocolo, *Intelligenza artificiale e giustizia*, cit.

[472] I *bias* sono errori cognitivi che l'intelligenza artifciale commette sulla base degli esempi che sono stati ad essa forniti. Per un approfondimento cfr. A. Turing, *Intelligenza meccanica*, Bollati Boringhieri, Torino, 1994.

sviluppo della tecnologia e delle sue applicazioni. Tale scopo può essere raggiunto assicurando che i sistemi di IA rispettino precisi criteri e requisiti messi a punto per il loro utilizzo.

La *reliability* viene citata nella prima appendice alla *Carta etica europea*, ponendola in rapporto alla qualità dei dati immessi nel sistema di IA: essa dipende strettamente «*on the quality of the data used and the choice of machine learning technique*»[473].

Nella nuova proposta di regolamento, invece, l'affidabilità, seppur sia solo richiamata, sembra invece acquisire la connotazione di un vero e proprio requisito per un sistema di IA "ad alto rischio", qualora sia utilizzato in un contesto di *law enforcement*, al fine di «*adverse impacts, retain public trust and ensure accountability and effective redress*»[474].

Insomma, dall'analisi dei tre documenti emerge una certa comunanza di intenti, da parte delle istituzioni dell'Unione europea e del Consiglio d'Europa, nel voler regolamentare in modo "etico" l'utilizzo dell'IA: le numerose e recenti iniziative normative evidenziano un'annunciata svolta epocale, soggetta ad un continuo bilanciamento fra innovazione e protezione dei diritti fondamentali dell'individuo. La scelta sovranazionale di ricorrere a strumenti giuridici ed etici adeguati appare l'unica via oggi percorribile per consentire di governare efficacemente i mutamenti significativi che influenzeranno la vita individuale e sociale delle persone.

3. Tecniche di intelligenza artificiale applicate alla disciplina biometrica

3.1 Sistemi di riconoscimento biometrico e normativa europea: un "percorso di conformità" alla proposta di regolamento

Come già accennato poc'anzi[475], con riferimento ai sistemi di identificazione biometrica, la nuova proposta di regolamento ha introdotto un insieme di norme che, seppur si ritengano ancora per certi versi troppo vaghe e, a tratti, sibilline, appaiono, in ultima analisi abbastanza soddisfacenti, segnando in ogni caso una svolta epocale in termini di completezza del *framework* normativo europeo. A questo punto della trattazione vale quindi la pena soffermarsi sugli aspetti della regolamentazione più rilevanti e specificamente concernenti il complesso ambito dei sistemi di riconoscimento biometrico. La nuova proposta di regolamento ha adottato una definizione di "dato biometrico" del tutto coerente con quella introdotta dall'art. 4(14) del GDPR, dall'art. 3(18) del regolamento (UE) 2018/1725 e dall'articolo 3(13) della LED. In particolare, si definiscono tali «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una

[473] Cfr. CEPEJ, *Appendix I – In-depth study on the use of AI in judicial systems*, cit. p. 32.
[474] Cfr. il considerando n. 38, EUROPEAN COMMISSION, *Proposal for a Regulation,* cit., p. 27.
[475] Cfr. il § 2.1.1.

persona fisica che ne consentono o ne confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»[476]. In linea con i succitati documenti normativi, rimarrebbero fuori le fotografie ritraenti dati biometrici, ad eccezione di quelle trattate attraverso un dispositivo tecnico specifico «che consente l'identificazione univoca o l'autenticazione di una persona fisica»[477].

Più nel dettaglio, la proposta diversifica sapientemente due modalità di utilizzo di un sistema di riconoscimento biometrico[478]: *real time* e *post remote* (cfr. *infra* lo schema n. 4)[479]. Il primo viene definito come «*an AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used*»[480]. Trattasi, quindi, di un procedimento automatizzato finalizzato a stabilire o confermare l'identità di un determinato soggetto a distanza. Tenuto conto delle diverse caratteristiche e modalità applicative, nonché dei diversi rischi per i diritti fondamentali connessi, la proposta di regolamento tiene separato l'ambito dei sistemi di riconoscimento biometrico che funzionano a posteriori (cfr. il cap. I, § 1.1), affermando che «*in the case of 'post' systems, in contrast, the biometric data have already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned*»[481]. Si ritiene che tale ultima espressione andrebbe ulteriormente specificata per non lasciarne all'interprete una lettura ambigua. Infatti, per potersi dire coerente con il precedente *framework* normativo europeo (cfr. *supra*), all'espressione «*pictures or video footage generated by closed circuit television cameras or private devices*» dovrebbe essere aggiunta l'ulteriore specificazione dell'applicazione di un dispositivo tecnico specifico che consenta successivamente l'identificazione o l'autenticazione univoca di una persona fisica (cfr. il capitolo I, § 1).

Entrambe le modalità di impiego dei sistemi di riconoscimento biometrico rientrano nella categoria ad "alto rischio" (cfr. *infra* schema n. 4)[482]. Non si comprende però la ragione per cui l'impiego dei

[476] Cfr. art. 4(14), GDPR, cit.

[477] Cfr il considerando n. 51, GDPR, cit. e considerando n. 21, regolamento (UE) 2018/1725.

[478] Cfr. il cap. I, § 1.1.

[479] In entrambi i casi si considerano solamente i sistemi di riconoscimento "*remote*", escludendo pertanto quelli che richiedono un contatto fisico con un sensore.

[480] Cfr. il considerando n. 8, EUROPEAN COMMISSION, *Proposal for a Regulation,* cit.

[481] Cfr. il considerando n. 8, EUROPEAN COMMISSION, *Proposal for a Regulation,* cit.

[482] Il Parlamento europeo, peraltro, tramite il COMMITTEE ON LEGAL AFFAIRS FOR THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION AND THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft Opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts* (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 2.3.2022, ha proposto di escludere specificamente dai sistemi ad "alto rischio" quelli che permettono una «*biometric authentication, of*

sistemi "*real time*", in spazi aperti al pubblico, da parte delle autorità di *law enforcement*, sia vietata, salve le eccezioni già richiamate, mentre un loro utilizzo da parte di un privato sia da intendere solo come ad "*high risk*"[483].

La proposta di regolamento per la prima volta compie un passo avanti rispetto alla precedente regolamentazione. Nella categoria delle tecniche di IA ad alto rischio vengono annoverati altresì i cd. "sistemi di riconoscimento delle emozioni", ossia strumenti in grado di interpretare gli stati d'animo e le intenzioni delle persone fisiche sulla base dei loro dati biometrici[484]. Trattasi di strumenti particolarmente intrusivi della sfera personale del singolo (come per es. il cd. "*lie detector*"[485]) che devono rispettare diversi parametri di riferimento per potersi considerare *compliant* rispetto alla normativa in esame. In particolare, gli artt. 6 e ss. prescrivono una serie di requisiti obbligatori che devono essere rispettati per poter immettere nel mercato dell'Unione europea sistemi di tal guisa, posto che essi siano compatibili con le più stringenti disposizioni normative interne. Infatti, secondo quanto stabilito dal considerando n. 27, la *ratio* dell'introduzione di tali prerogative consisterebbe nella funzione di garantire un impiego etico e sicuro di taluni sistemi di IA che, a seconda della loro finalità di utilizzo, potrebbero avere un impatto potenzialmente nocivo per i diritti fondamentali[486],

---

natural persons (i.e., revealing their identity or tracking their behaviour)without their expressed or implied agreement» (Cfr. *Annex III – paragraph 1 – point 1 – introductory part*).

[483] Cfr. N. A. Smuha, E. Ahmed Rengers, A. Harkens, W. Li, J. MacLaren, R. Piselli, K. Yeung, *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, 2021, reperibile all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991 (visualizzato in data 20.2.2022). Il Parlamento europeo, peraltro, tramite il COMMITTEE ON LEGAL AFFAIRS FOR THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION AND THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft Opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts* (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 2.3.2022, ha proposto di specificare che «(…) *'real-time' and 'post' remote biometric identification systems should be classified as high-risk, except for the purpose of remote client on-boarding or authentication of a user though a device*».

[484] Cfr. l'art. 3 (34), EUROPEAN COMMISSION, *Proposal for a Regulation*, cit. Trattasi di sistemi utilizzati con lo scopo di riconoscere le emozioni e gli stati d'animo degli individui e non a fini di riconoscimento: per tale ragione non saranno oggetto di approfondimento della presente ricerca. Il Parlamento europeo, tramite il COMMITTEE ON LEGAL AFFAIRS FOR THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION AND THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft Opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts* (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 2.3.2022, p. 30, ha proposto di emendare la definizione come segue «*'emotion recognition system' means an AI system for the purpose of identifying or inferring emotions of natural persons on the basis of their biometric or other data obtained, read or interpreted from an individual*».

[485] Trattasi di uno strumento che registra le modificazioni del respiro, del polso e della pressione arteriosa allo scopo di obiettivare le reazioni emotive concomitanti alla formulazione di risposte menzognere. Su questo strumento cfr. *ex multis* G. Fisher, The Jury's Rise as Lie Detector, 107 in *YALE L.J.* 575 (1997) e W.G. Iacono, D.T. Lykken, *The validity of the lie detector: Two surveys of scientific opinion*, in *Journal of Applied Psychology*, 82(3), 1997, 426–433.

[486] I diritti fondamentali interessati in questo ambito concernono la dignità umana, il rispetto della vita privata e familiare, la protezione dei dati personali, la libertà di espressione e di informazione, la libertà di riunione e di associazione, la non discriminazione, la protezione dei consumatori, i diritti dei lavoratori, i diritti delle persone con disabilità, il diritto a un ricorso effettivo e a un processo equo, il diritto alla difesa, la presunzione di innocenza e il diritto ad una buona amministrazione. Oltre a questi diritti, giova ricordare che i bambini godono di specifici diritti salvaguardati dall'art. 24 della *EU Charter of fundamental rights*. Cfr. il considerando n. 28, EUROPEAN COMMISSION, *Proposal for a Regulation*, cit.

per la salute o per la sicurezza delle persone. Per tale ragione, la Commissione europea ritiene importante che i rischi per i diritti fondamentali che possono essere generati da un prodotto di IA nel suo complesso[487] debbano essere debitamente prevenuti e, ove possibile, attenuati[488]. Tuttavia, ancora una volta[489], vien da domandarsi se l'introduzione di una serie di requisiti tecnici, ai quali i software di IA devono risultare conformi, possa ritenersi di per sé sufficiente per garantire un'adeguata protezione dei diritti fondamentali dell'individuo. Il rischio che si corre è che la predisposizione di una serie di criteri, anche molto dettagliati, cui occorre attenersi per la progettazione e l'impiego di determinati strumenti sostituisca una tutela effettiva da parte dell'Unione europea. Risultano, infatti, del tutto assenti prescrizioni positive aventi ad oggetto i diversi potenziali responsabili e i rimedi in caso di eventuali trasgressioni[490].

Il criterio teleologico risulta poi particolarmente interessante e flessibile per gli sviluppi tecnologici futuri: esso tiene conto non solo della potenziale gravità del danno morale o materiale arrecato da un utilizzo improprio di tali sistemi di IA "ad alto rischio", ma anche della possibilità empirica del suo verificarsi. Per quanto concerne i sistemi di riconoscimento biometrico, quindi, con riferimento a entrambe le modalità applicative, il considerando n. 33 sottolinea i possibili risultati distorti e potenzialmente discriminatori: per tale ragione, entrambe le modalità d'impiego devono essere considerate "ad alto rischio", soggette quindi ad una serie di requisiti obbligatori che si approfondiranno meglio *infra*. In tal senso, anche i sistemi di IA destinati più in generale all'amministrazione della giustizia sarebbero da ricondurre nella stessa categoria[491], tenuto conto del

---

[487] Intesi sia come componente "ad alto rischio" installato su un determinato sistema sia come sistema autonomo unico. Cfr. il considerando n. 30, EUROPEAN COMMISSION, *Proposal for a Regulation,* cit.

[488] Cfr. il considerando n. 28, EUROPEAN COMMISSION, *Proposal for a Regulation,* cit.

[489] Cfr. il § 2.1.1.

[490] Questa tendenza da parte del legislatore europeo è riscontrabile in generale, non solo con riferimento alla proposta di regolamento sull'IA. Sul punto cfr. A. Cabiale, *I limiti alla prova nella procedura penale europea*, cit., pp. 311 e 312, S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, cit., p. 76, M. Caianiello, *Dal terzo pilastro ai nuovi strumenti: diritti fondamentali, "road map" e l'impatto delle nuove direttive*, in *I nuovi orizzonti della giustizia penale europea, Atti del convegno*. Milano, 24-26 ottobre 2014, Milano, 2015, p. 112 e N. Smuha, E. Ahmed-Rengers, A. Harkens, W. Li, J. MacLaren, R. Piselli, K. Yeungg, *How the Eu can achieve legally trustworthy AI: a response to the European Commission's Proposal for an Artificial Intelligence Act*, reperibile all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991 (visualizzato in data 22.2.2022).
A tal proposito, il Parlamento europeo con la *resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL))* ritiene che «based on the legal challenges that AI-systems pose to the existing civil liability regimes, it seems reasonable to set up a common strict liability regime for those high-risk autonomous AI-systems» e, per tale ragione, «*requests the Commission to submit, on the basis of Article 225 of the Treaty on the Functioning of the European Union, a proposal for a Regulation on liability for the operation of Artificial Intelligence-systems, following the recommendations set out in the Annex hereto*». Su questo punto v. anche *Inception impact assessment* - Ares(2021)4266516 avente ad oggetto la "*Civil liability – adapting liability rules to the digital age and artificial intelligence*", reperibile all'indirizzo https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en (visualizzato in data 31.1.2022).

[491] Non solo quelli aventi scopi probatori ma anche quelli progettati come supporto alle decisioni dell'autorità giudiziaria, cfr. il § 2.

loro impatto potenzialmente lesivo sulla democrazia, sul principio di legalità, sulle libertà individuali e sul diritto ad un processo equo (cfr. il considerando n. 40).

Conformemente a quanto stabilito dal considerando n. 70, qualora un soggetto sia esposto all'interazione con un sistema di classificazione biometrica, dovrebbe essere sempre ragionevolmente informato, soprattutto se si tratta di persona affetta da una particolare disabilità. Sebbene non sia ulteriormente specificata la modalità di pubblicizzazione di tali informazioni, si ritiene comunque debba essere adeguata al raggiungimento dello scopo, quindi non troppo nascosta, per permettere che il testo dell'informazione sia ben visibile. La stessa disposizione normativa specifica per la prima volta un aspetto particolarmente interessante: i soggetti che utilizzano sistemi di IA per generare o manipolare contenuti di immagini, audio e video che assomigliano sensibilmente a determinate persone, devono essere consapevoli della provenienza totalmente artificiale di tali contenuti.

Venendo alle disposizioni introdotte per la regolamentazione dei sistemi di IA ad alto rischio, giova premettere che innanzitutto la regola generale per l'utilizzo delle tecniche di riconoscimento biometrico *tout court* è quella di una progettazione attenta alla valutazione della conformità ai requisiti di documentazione e sorveglianza umana. Le norme che regolano tutta la categoria di sistemi "ad alto rischio" [cfr. art. 6 e *Annex III-High risk AI Systems referred to in article* 6(2)] si rivolgono ai potenziali destinatari del ciclo produttivo di un sistema: fornitori, produttori, distributori e importatori (art. 2).

Come già anticipato poc'anzi (cfr. *supra*), quello che può essere definito come un "percorso di conformità" al testo del regolamento ha inizio con la delimitazione della specifica finalità per cui si utilizza lo strumento. A seconda dello scopo di destinazione di un determinato sistema di IA, sarà individuato un corrispondente livello di rischio per la salute, la sicurezza pubblica e le libertà fondamentali (cd. valutazione del rischio); conseguentemente, sarà aggiornato l'elenco dei *tools* presenti nell'appendice III della proposta (art. 7)[492].

[492] «*(…) the Commission shall take into account the following criteria: (a) the intended purpose of the AI system; (b) the extent to which an AI system has been used or is likely to be used; (c) the extent to which the use of an AI system has already caused harm to the health and safety or adverse impact on the fundamental rights or has given rise to significant concerns in relation to the materialisation of such harm or adverse impact, as demonstrated by reports or documented allegations submitted to national competent authorities; (d) the potential extent of such harm or such adverse impact, in particular in terms of its intensity and its ability to affect a plurality of persons; (e) the extent to which potentially harmed or adversely impacted persons are dependent on the outcome produced with an AI system, in particular because for practical or legal reasons it is not reasonably possible to opt-out from that outcome; (f) the extent to which potentially harmed or adversely impacted persons are in a vulnerable position in relation to the user of an AI system, in particular due to an imbalance of power, knowledge, economic or social circumstances, or age; (g) the extent to which the outcome produced with an AI system is easily reversible, whereby outcomes having an impact on the health or safety of persons shall not be considered as easily reversible; (h) the extent to which existing Union legislation provides for: (i) effective measures of redress in relation to the risks posed by an AI system, with the exclusion of claims for damages; (ii) effective measures to prevent or substantially minimise those risks*». EUROPEAN COMMISSION, *Proposal for a Regulation*, cit., art. 7.

Il procedimento di valutazione del rischio non dev'essere compiuto solo all'inizio dell'*iter* (art. 9, par. 2), ma dev'essere eseguito periodicamente. Una volta compreso, valutato e gestito il livello di rischio associato ad un determinato sistema di IA, dovrà essere rispettata tutta una serie di ulteriori requisiti. In primo luogo, la cd. *data governance* (art. 10), che garantisce che il sistema funzioni come ci si era prefigurati inizialmente: a tal proposito, i dati utilizzati per l'addestramento del sistema devono essere privi di errori, completi e pertinenti. Il rischio qui è che si verifichi il fenomeno di cd. *overfitting* del sistema in cui lo strumento conferisce eccessivo valore ai dati di *fitting* utilizzati per l'addestramento e l'algoritmo non è in grado di "generalizzare" adeguatamente per giungere ad un risultato affidabile. In ogni caso, l'art. 10 (par. 2) evidenzia la necessità di implementare dei metodi che prevengano la discriminazione di determinati gruppi di persone[493].

L'art. 11 prescrive che la documentazione tecnica debba essere redatta prima dell'immissione sul mercato o della messa in servizio del *tool*: essa dev'essere oggetto di un costante aggiornamento e riportare tutte le informazioni necessarie per la valutazione di conformità ai requisiti del regolamento. È stata prevista, poi, *ex* art. 12, la possibilità di una registrazione automatica degli eventi (tramite il cd. *log*) durante il funzionamento dei sistemi di IA: in questo modo viene garantito un elevato livello di tracciabilità durante l'intero ciclo di vita dello stesso. Gli eventi che possono essere registrati concernono essenzialmente circostanze che possono comportare un rischio per la salute, la sicurezza o la protezione dei diritti fondamentali delle persone, ovvero una modifica sostanziale di un dato o di un risultato scaturente dal sistema. Con riferimento al requisito della trasparenza, l'art. 13, come già visto *supra* al § 2.2, prescrive che gli utenti devono essere in grado di capire la logica sottesa al funzionamento degli algoritmi. Non solo il linguaggio utilizzato deve essere chiaro, ma è necessario anche rendere consapevoli gli utenti dei possibili rischi connessi all'impiego di un sistema di IA. L'articolo 14 invece regola l'ambito della cd. *human oversight*, prevedendo - ad una certa fase del procedimento di impiego del sistema - una verifica/controllo da parte di un operatore esperto al fine di prevenire o ridurre al minimo i rischi per la salute, la sicurezza pubblica o i diritti fondamentali.

Infine, è stato introdotto uno specifico obbligo di *accuracy, robustness and cybersecurity*, rispetto ai rischi concernenti i limiti di un sistema di IA (per un approfondimento cfr. *supra*, il § 2.2).

---

[493] Il Parlamento europeo, tramite il COMMITTEE ON LEGAL AFFAIRS FOR THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION AND THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft Opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, cit., p. 56, ha specificato che «*in assessing the quality of a data set, account shall be taken to the extent to which the data set is constructed with a view to fulfilling in particular the following aspects: a) provides a similar output for relevant demographic Groups impacted by the system; b) minimizes disparities in outcomes for relevant demographic groups impacted by the system, in case where the system allocates resources or opportunities to natural persons; c) minimizes the potential for stereotyping, demeaning, or erasing relevant demographic groups impacted by the system where the system describes, depicts, or otherwise represents people, cultures, or society*» (art. 10, par. 3).

La seconda modalità di utilizzo dei sistemi di riconoscimento biometrici è quella in *real time*, per i quali, se utilizzati da autorità di *law enforcement* in spazi aperti al pubblico, *ex* art. 5, par. 1, lett. *d*), si prescrive un divieto di impiego, fatta eccezione per una serie di casi espressamente previsti dalla stessa disposizione. A tal proposito, giova richiamare l'art. 3(40) che definisce l'autorità incaricata dell'applicazione della legge come «*any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties*», comprese quelle competenti per la salvaguardia da minacce alla sicurezza pubblica (lett. *a*). Nella nozione rientra altresì qualsiasi organismo, o entità, incaricato dal diritto dell'Unione europea di esercitare poteri pubblici ai fini della prevenzione, dell'indagine, dell'accertamento o del perseguimento dei reati (lett. *b*)[494].

La portata dell'espressione di "spazio accessibile al pubblico" appare piuttosto circoscritta, stabilendo il considerando n. 9 che con esso s'intenda qualsiasi luogo fisico accessibile al pubblico, a prescindere dal fatto che sia di proprietà privata o pubblica. La nozione, pertanto, non ricomprenderebbe i luoghi generalmente non accessibili a terzi, comprese le autorità di *law enforcement*, fatta eccezione per il caso in cui siano state espressamente autorizzate (per es. abitazioni, club privati, uffici, magazzini e fabbriche). Inoltre, nella definizione non v'è spazio nemmeno per i luoghi "online", non potendoli considerare come "fisici". In ogni caso, la bozza di regolamento suggerisce che, a scanso di equivoci, l'accessibilità pubblica ad un determinato spazio sia da determinare caso per caso, tenendo conto delle specificità della fattispecie concreta[495].

L'articolo 5, poi, specifica alcune circostanze in cui l'impiego della tecnologia in esame risulta «*strictly necessary*», elencando i casi in cui è consentito l'utilizzo di un sistema di riconoscimento basato su tecniche di IA in modalità *real time*. In particolare, come già accennato in precedenza, la disposizione stabilisce le seguenti eccezioni:

I. la ricerca mirata di potenziali vittime di reato, compresi i minori scomparsi;
II. la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o la sicurezza pubblica delle persone fisiche o di un attacco terroristico;
III. l'individuazione, la localizzazione, l'identificazione o il perseguimento dell'indagato o dell'autore (se già accertato), di uno dei reati previsti dall'articolo 2(2) della decisione quadro

[494] Il Consiglio dell'Unione europea con un primo testo di modifica delle disposizioni contenute nella proposta di regolamento della Commissione europea (COUNCIL OF THE EUROPEAN UNION, *Presidency compromise text*, 2021/0106(COD), 29.11.2021 ha proposto di specificare che che tali sistemi di IA potrebbero essere utilizzati anche da altri soggetti che agiscono per conto delle autorità di contrasto o collaborano con esse. Il Parlamento europeo, tramite il COMMITTEE ON LEGAL AFFAIRS FOR THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION AND THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft Opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts* (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 2.3.2022, ha ribadito tale concetto proponendo di aggiungere all'art. 5, par. 1 «*by law enforcement authorities or on their behalf for the purpose of law enforcement*».

[495] Cfr. il considerando n. 9, EUROPEAN COMMISSION, *Proposal for a Regulation*, cit.

2002/584/JHA62 e punibile nello Stato membro interessato con una pena della reclusione nel massimo fino a tre anni, secondo la legge di quello specifico Stato membro[496].

Nel successivo paragrafo, si aggiunge che l'utilizzo dei sistemi *de quibus* dovrà inoltre essere ponderato sulla base della «natura della situazione» nonché sulle «conseguenze» che possono derivarne «per i diritti e le libertà di tutte le persone interessate», con particolare riguardo, nel primo caso, alla «gravità», alla «probabilità» ed all'«entità del danno causato dal mancato uso del sistema» (a) e, nella seconda ipotesi, alla «gravità», alla «probabilità» ed all'«entità» delle suddette conseguenze (b). Viene inoltre operato un riferimento esplicito alla necessità di stabilire limitazioni «temporali» e «geografiche», oltreché «personali», che siano «necessarie e proporzionate in relazione all'uso». In tutti questi casi, secondo la Commissione, l'impiego di questi strumenti sarebbe giustificato da ragioni rilevanti di pubblica sicurezza.

Per vero, emergono sin da una prima lettura alcuni dubbi interpretativi circa l'applicazione pratica del regolamento in questi termini[497]. Quante volte, in occasione per esempio di grandi assembramenti, abbiamo avuto la sensazione di essere in presenza di una minaccia "sostanziale e imminente"? In quali occasioni potremmo essere sicuri di poter trovare una "potenziale vittima di reato" o un "bambino scomparso"? Anche un minimo sospetto della presenza di potenziali vittime della criminalità, in un luogo geograficamente determinato, potrebbe spingere un organo di polizia giudiziaria, durante la fase delle indagini preliminari, ad attivare il meccanismo in *real time*, mettendo potenzialmente a rischio plurimi diritti fondamentali nei confronti di molteplici soggetti.

Stesso discorso per la ricerca di minori scomparsi. Il limite della previsione allora consisterebbe in una mancata puntuale delimitazione del concetto di "sospetto" da parte di un'autorità che legittimamente possa servirsi di un sistema di identificazione simultaneo. Il rischio, ad oggi, è che qualsiasi dubbio sull'esistenza delle predette circostanze possa condurre ad un'indiscriminata sorveglianza di massa. Infatti, il sistema di riconoscimento in *real time*, funzionando su larga scala, può riguardare anche persone presenti a manifestazioni politiche e sociali o grandi eventi, che non sono in alcun modo oggetto di "attenzione" da parte delle forze di polizia.

Peraltro, anche il secondo caso, sebbene la minaccia descritta debba essere «*specific, substantial and imminent*», risulterebbe eccessivamente discrezionale e poco attenta ai possibili utilizzi distorti da parte delle autorità di pubblica sicurezza. Rispetto alla regolamentazione di questa seconda modalità di utilizzo dei sistemi di riconoscimento biometrico, si ritiene che la base di partenza sia

[496] La decisione quadro 2002/584/JHA62 è reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002F0584 (visualizzato in data 11.5.2021).

[497] Cfr. M. Ebers, V.R.S. Hoch, F. Rosenkranz, H. Ruschemeier, B. Steinrötter, *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society*, in *(RAILS). J.* 2021, 4(4), pp. 589-603.

opportuna, ma le disposizioni non appaiono ancora sufficientemente precise nella loro formulazione, potendo provocare nel tempo interpretazioni estensive, a danno delle libertà fondamentali della popolazione dei diversi Stati membri.

Oltre a questo, anche la terza eccezione potrebbe essere di complessa applicazione, dal momento che la gravità del reato, per permettere l'attivazione del sistema automatico, è valutata in base al massimo della pena edittale prevista per un determinato reato, che cambia, anche per le stesse qualificazioni delle fattispecie astratte, nei vari Stati membri. Questo potrebbe portare a disparità di trattamento con conseguenti potenziali problematiche nell'ottica della cooperazione giudiziaria e di polizia[498]. Infatti, potrebbe esserci il rischio che l'impiego dello strumento in questa modalità applicativa sia consentito in uno Stato e non sia, per la stessa fattispecie di reato, attivabile in un altro Stato membro. Oltretutto, la proposta lascia ai singoli Stati membri la facoltà di decidere se attuare o meno le suddette eccezioni per l'impiego dei *tools* di riconoscimento tramite specifiche leggi nazionali.

Da accogliere con favore è, invece, la previsione collocata nel par. 3 che, per l'utilizzo di tali sistemi di IA, richiede necessariamente un'autorizzazione preventiva da parte di un'autorità giudiziaria, salvi i casi di particolare urgenza in cui la stessa potrà essere data successivamente. Spetterà poi a ciascuno Stato membro, in base al proprio diritto nazionale, specificare ulteriormente il procedimento per la richiesta e l'emissione dell'autorizzazione da parte dell'autorità giudiziaria (art. 5, par. 4). Occorre accertare, pertanto, sulla base di «prove oggettive» o «indicazioni chiare», la necessità e la proporzionalità della misura rispetto ad almeno una delle finalità ammesse. L'unica ipotesi in cui risulta consentito prescindere dall'autorizzazione riguarda eventuali situazioni di urgenza, salva in ogni caso la necessità di ottenere la convalida (§ 3). L'unico profilo di rischio, connesso all'applicazione di tale disposizione, concerne il grado di indipendenza della magistratura che non risulta allo stesso livello per ciascuno Stato membro. In tal senso, la norma potrebbe rivelarsi nel tempo completamente inutile e soggetta ai cambi di governo operati nei diversi Stati.

Quanto ai sistemi di categorizzazione biometrica, essi sono stati definiti come quei *tools* di IA che impiegano i dati biometrici di persone fisiche «al fine di assegnarle a categorie specifiche, quali quelle basate sul sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, l'origine etnica o l'orientamento sessuale o politico»[499]. Non essendo classificati come sistemi "ad alto rischio", essi sarebbero soggetti solamente alle regole di trasparenza concernenti le informazioni sul funzionamento del sistema da fornire alle persone fisiche che vi sono esposte. Orbene, si ritiene tale proposta di

[498] Cfr. su questo punto A. Lavorgna, G. Suffia, *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2/2021, pp. 88 e ss.
[499] Cfr. l'art. 3 par. 35, 2021/0106(COD).

classificazione, anche sotto questo punto di vista, piuttosto discutibile. Infatti, la distinzione fra sistema impiegato a fini di categorizzazione e a fini di riconoscimento rischia di diventare una *quaestio* puramente arbitraria. L'impiego in spazi aperti al pubblico di sistemi di categorizzazione biometrica potrebbe avere un impatto altrettanto negativo sui diritti fondamentali degli individui[500]. A titolo esemplificativo, è stato evidenziato come questi sistemi potrebbero essere utilizzati dalle autorità di polizia per «*classifying people in public places as of a certain ethnicity or political orientation*», posto che «*they are under no obligation to include human oversight, or to notify people that the system is in use*»[501]. A tal proposito, l'*European Data Protection Supervisor* (EDPS) sostiene che si dovrebbe adottare un approccio più rigoroso per la regolamentazione dell'impiego del riconoscimento automatizzato in spazi aperti al pubblico, indipendentemente che questi siano utilizzati in un contesto commerciale, amministrativo o di *law enforcement*[502]. Infatti l'EDPS, insieme all'*European Data Protection Board* (EDPB), in un parere congiunto non vincolante ha proposto un «*general ban on any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals - in any context*»[503], dal momento che «*problem regarding the way to properly inform individuals about this processing is still unsolved*»[504]. Oltre a ciò, «*the intrusiveness of the processing does not always depend on the identification being done in real-time or not. Post remote biometric identification in the context of a political protest is likely to have a significant chilling effect on the exercise of the fundamental rights and freedoms, such as freedom of assembly and association and more in general the founding principles of democracy. Second, the intrusiveness of the processing does not necessarily depend on its purpose. The use of this system for other purposes such as private security represents the same threats to the fundamental rights of respect for private and family life and protection of personal data*»[505].

La proposta costituisce certamente un buon punto di partenza. Vi sono però alcune criticità che potrebbero emergere in fase applicativa qualora il testo normativo non dovesse subire modifiche o

[500] Cfr. sul punto G. Malgieri, M. Ienca, *The EU regulates AI but forgets to protect our mind*, 7.7.2021, reperibile all'indirizzo https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/ (visualizzato in data 20.1.2022).

[501] Cfr. C. Kind, *Containing the canary in the AI coalmine – the EU's efforts to regulate biometrics*, in *Ada Lovelace Institute*, 2021, reperibile all'indirizzo https://www.adalovelaceinstitute.org/blog/canary-ai-coalmine-eu-regulate-biometrics/ (visualizzato in data 20.1.2022).

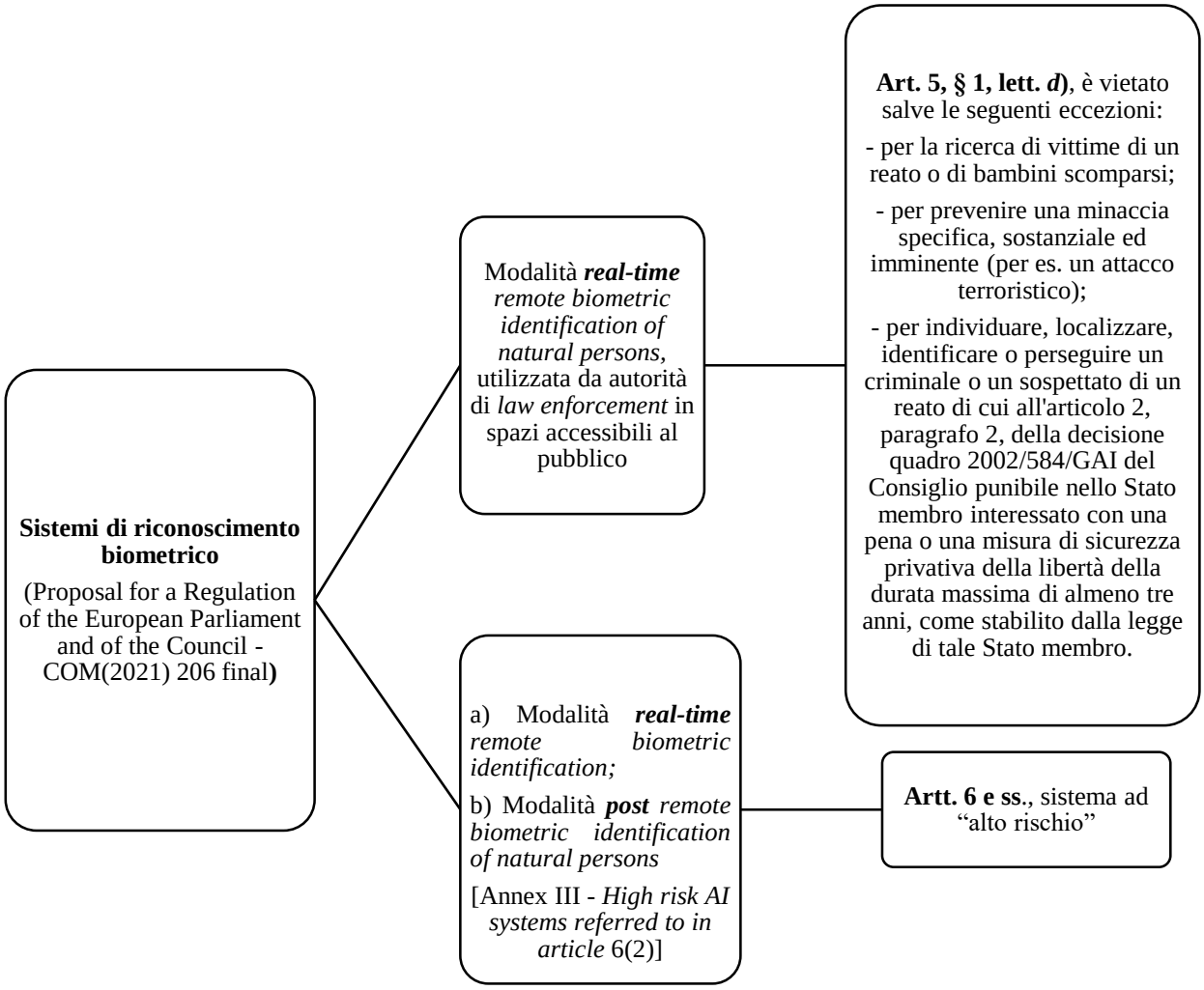
[502] Cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary*, 2021, reperibile all'indirizzo https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en (visualizzato in data 20.1.2022).

[503] Cfr. EDPB – EDPS, *Joint opinion 5/2021*, 18.6.2021, p. 3, reperibile all'indirizzo https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf (visualizzato in data 20.1.2022).

[504] Cfr. EDPB – EDPS, *Joint opinion 5/2021*, 18.6.2021, cit., p. 12.

[505]Cfr. EDPB – EDPS, *Joint opinion 5/2021*, 18.6.2021, cit., p. 12.

integrazioni[506]. Come evidenziato, sarà interessante comprendere come le diverse eccezioni al divieto del riconoscimento in modalità "*real time*" da parte delle autorità di *law enforcement* in spazi aperti al pubblico opereranno in concreto e come l'interpretazione del regolamento ne verrà di riflesso condizionata.



Schema n. 3

4. Alcune riflessioni conclusive

Con il presente capitolo, sono stati operati significativi inquadramenti della rappresentazione digitalizzata di un dato biometrico e del suo modello elettronico. In particolare, si è inteso

[506] Giova ricordare che, in data 6.10.2021, in occasione della pubblicazione della Risoluzione 2020/2016(INI) - "*Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*", il Parlamento europeo ha votato per richiedere una moratoria sull'adozione di sistemi di riconoscimento facciale a fini identificativi, salvo il loro impiego per il riconoscimento di vittime di reato, fino a quando non vi sarà una normativa di riferimento che attesti la conformità di tali sistemi ai diritti fondamentali e vi saranno prove empiriche della necessità e della proporzionalità per la diffusione dell'impiego di tali tecnologie. Sulla base di questo documento, è già posibile prevedere che il testo della proposta subirà importanti modifiche.

ricomprendere il trattamento del dato biometrico digitalizzato entro alcune prime categorie dogmatiche processuali tradizionali, fornendo al lettore specifici parametri che saranno utili per la comprensione dell'analisi dell'impiego di sistemi di riconoscimento biometrici automatizzati nello spettro delle garanzie processuali fondamentali (cfr. *infra* il capitolo III). Rispetto ad essi, è bene rimanere consapevoli dei "diversi livelli di complessità"[507] che pone il dato biometrico *tout court*, considerata l'intrinseca specificità delle fonti di prova in esame. Infatti, la rivoluzione digitale ha offuscato i limiti e i contorni tra le diverse aree di studio senza precedenti. Si tratta di *step* di complessità successivi rispetto alle questioni tradizionali esistenti tra scienza e giustizia penale. Come già sottolineato nel capitolo I, i tratti biometrici sono rispondenti a principi e misurazioni che attingono alle più differenti discipline: dalla biologia alla statistica, dalla fisica all'informatica. Ma si tratta solo del livello più basilare di complessità. Su questo si innesta infatti la natura digitale del dato. Ciò che accomuna le diverse tipologie sopra descritte e le molteplici definizioni di *digital evidence* è proprio la fondamentale caratteristica del dato da cui trarre l'informazione probatoria: la sua materialità non immediatamente percepibile. E con essa tutti i consueti tratti di immaterialità, dispersione, promiscuità e congenita modificabilità. Tuttavia, nonostante le analogie sussistenti tra le due categorie di dato, in un rapporto di *genus* a *species*, vien da domandarsi se le regole previste per la *chain of custody* del dato digitale siano adeguate a garantire l'affidabilità del tratto biometrico digitalizzato, il quale, come visto, presenta ulteriori profili di complessità derivanti dalle sue caratteristiche ontologiche instrinseche (cfr. il capitolo I). Potrebbe risultare più efficace a questo punto pensare ad un'apposita "*biometric chain of custody*", tenendo conto delle analogie con la *digital evidence* (cfr. *supra*, §§ 1 e 1.1) e rispettando le peculiarità della disciplina alla base e le differenze fra i diversi tratti biometrici considerati (cfr. il capitolo I).

Entro tale contesto di complessità si colloca l'ulteriore livello di difficoltà, posta la diffusione applicativa di strumenti automatizzati al fenomeno processuale penale. È chiaro che l'identificazione, o l'autenticazione di un individuo, siano oltremodo agevolati dall'impiego di *tools* automatizzati, che consentono di estrarre automaticamente caratteristiche fisionomiche non direttamente visibili, rendendo agevoli confronti e valutazioni metriche. In tal senso, il vantaggio per il lavoro degli investigatori sul piano sia della velocità sia dell'efficienza è davvero sorprendente. Tuttavia, molto più di quanto sia possibile osservare nel territorio nazionale, a livello mondiale l'applicazione di tecniche di intelligenza artificiale al riconoscimento biometrico costituisce – oggi più che mai – un tema estremamente dibattuto. Per vero, come visto *supra*, i sistemi di IA possono restituire risultati fuorvianti per problemi di "apprendimento", ossia per un trattamento non corretto dei dati considerati

[507] Cfr. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, p. 226.

nella fase preliminare in cui il software elabora i propri modelli decisori (cd. "*training data*") ovvero per la cd. "discriminazione statistica", ossia l'esistenza di condizionamenti causati da rilevazioni statistiche effettuate precedentemente.

Come si approfondirà meglio *infra*, al capitolo III, l'introduzione sistematica di mezzi di riconoscimento biometrico all'interno del processo penale, potrebbe, 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.

La complessità del tema è evidente. La sovrapposizione fra diverse discipline e tematiche correlate sembra materializzare l'effettiva percezione di molteplici questioni che sono ancora da definire completamente. I diversi documenti normativi provenienti dall'Unione europea evidenziano uno sforzo significativo ma forse non ancora completo per l'individuazione e la riduzione al minimo dei rischi connessi all'impiego di tali controversi mezzi di riconoscimento.

Peraltro, l'eterogeneità dei profili professionali coinvolti nel dibattito pone in luce la complessità e la maturità scientifica con cui si sta studiando l'argomento. Il raggiungimento di una piena regolamentazione dei dati biometrici digitalizzati e il futuro dell'impiego dei sistemi di identificazione biometrica dipenderà oltremodo da questa auspicata cooperazione fra diversi settori disciplinari, tenendo sempre bene a mente i diritti fondamentali dell'individuo. Suona allora quanto mai profetica e d'ispirazione per la lettura dei paragrafi che seguiranno, un'altra significativa riflessione di Stefano Rodotà al proposito[508]: «l'unità della persona può essere ricostruita solo estendendo al corpo elettronico il sistema di garanzie costruito per il corpo fisico»[509].

[508] Una prima riflessione è riportata *supra* al § 1.4.2.

[509] Cfr. S. Rodotà, *Trasformazioni del corpo*, in *Politica del diritto*, 1, 2006, pp. 3-24.

CAPITOLO III

"*POLICY BEFORE TECHNOLOGY*": L'IMPIEGO DEGLI *AUTOMATED BIOMETRIC RECOGNITION SYSTEMS* NELLO SPETTRO DELLE GARANZIE FONDAMENTALI DELLA PERSONA*

«Legum servi sumus, ut liberi esse possimus»[1].

(MT Cicerone)

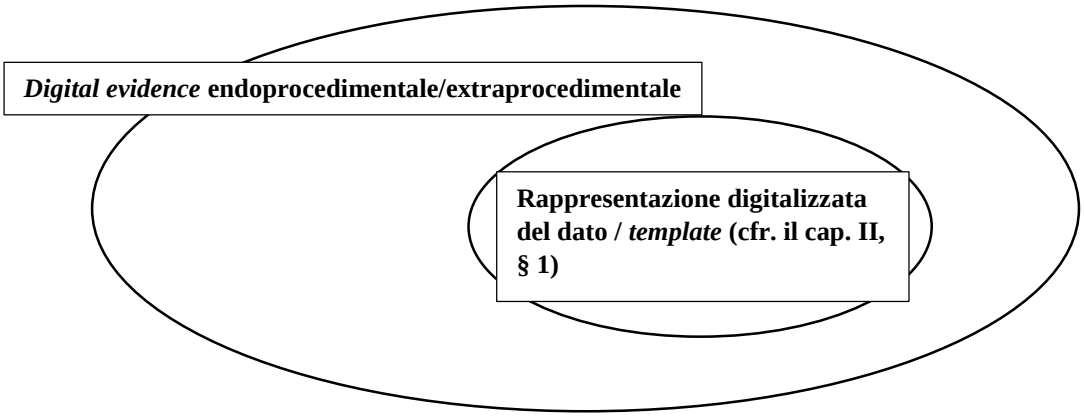
SOMMARIO: - 1. Considerazioni introduttive: l'impatto sui diritti fondamentali. - 1.1. Prova, scienza e processo penale: un trinomio in continua evoluzione. - 1.1.1. Il ruolo di un "*automated biometric match*" per l'accertamento del fatto di reato. - 1.1.2. Le indagini preliminari come *sedes materiae* degli strumenti tecnico-scientifici. - 1.2. *Digital evidence* e prova scientifica. - 1.3. Il *match* fra due dati biometrici digitalizzati come oggetto di prova. - 1.3.1. Il trattamento del dato biometrico digitalizzato tra accertamenti tecnici ripetibili in fase di indagini preliminari e prova in dibattimento. - 1.3.2. Il procedimento probatorio: l'ammissione del dato biometrico digitale generato automaticamente. - 1.3.3. L'assunzione. - 1.3.4. La valutazione. - 1.3.5. La decisione sul dato biometrico digitalizzato. - 2. Le coordinate costituzionali e i principi fondamentali nel trattamento di sistemi di riconoscimento automatizzati. - 2.1. Il dato biometrico digitalizzato e la libertà personale. - 2.1.1. Il prelievo coattivo di campioni biologici e la libertà personale. - 2.1.2. Riconoscimento facciale e libertà personale. - 2.1.3. Impronte digitali e libertà personale. - 2.1.4. Impronta fonica e libertà personale. - 2.2. Il dato biometrico digitalizzato e la parità delle armi. - 2.3. Il principio del *nemo tenetur se detegere*. - 2.4. Il trattamento del dato biometrico digitalizzato nel rispetto del diritto alla riservatezza. - 3. Alcune riflessioni conclusive.

* Il presente capitolo è costituito in parte da contributi già pubblicati, v. E. Sacchetto, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2/2019, E. Sacchetto, *Biometrics as forensic evidence: some reflections from the Italian Criminal proceeding's point of view*, in *8th International Workshop on Biometrics and Forensics (IWBF)*, 2020, E. Sacchetto, *Face to face*: i*l complesso rapporto tra automated facial recognition technology e processo penale*, in *www.lalegislazionepenale.it*, 16.10.2020.

[1] Marco Tullio Cicerone, *Pro Cluentio*, 66 a.C.

1. Considerazioni introduttive: l'impatto sui diritti fondamentali

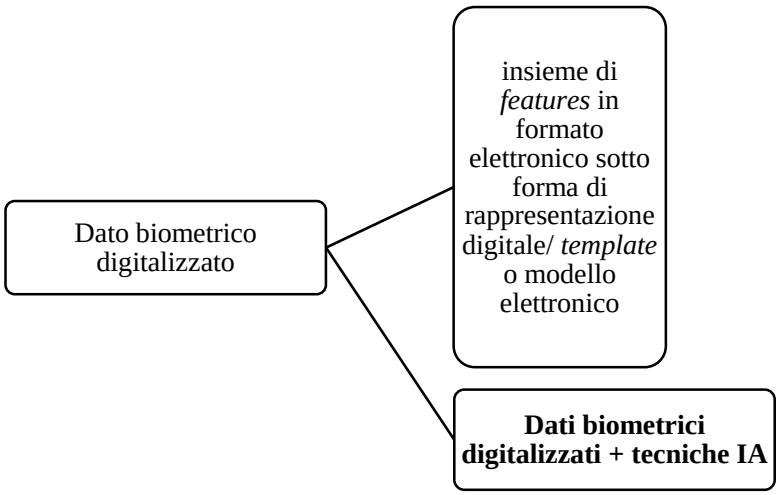
Si ricorda brevemente che il dato biometrico digitalizzato - ricondotto in via esegetica nelle categorie di *digital evidence* extraprocedimentale ed endoprocedimentale (cfr. *supra* il capitolo II, § 1) può i) trovarsi sotto forma di *template* ovvero di rappresentazione digitale di uno specifico tratto, ii) essere ricavato da un video o una fotografia digitale, ovvero iii) costituire la derivazione di dati generati automaticamente per un uso estraneo al procedimento penale, quali assistenti domestici o dispositivi elettronici di rilevamento delle caratteristiche fisiologiche e/o comportamentali[2]. In tutti questi casi, il dato può essere impiegato in un successivo momento per il confronto con altri modelli biometrici o rappresentazioni digitalizzate, senza dover necessariamente ricorrere ai dati grezzi da cui viene estratto[3].



Schema n. 1

Tale comparazione può essere eseguita tramite l'impiego di software che, grazie all'applicazione di processi automatizzati[4], effettuano calcoli probabilistici circa la corrispondenza tra un determinato dato e quello presente all'interno di un database. Come visto, il sistema, una volta avviata la ricerca, restituisce un certo numero di risultati, la cui quantità può – generalmente – essere prestabilita (cfr. il capitolo I, § 2.3).

[2] Cfr. il capitolo II, schema n. 1.
[3] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, p. 33.
[4] Tra i quali spiccano, per la particolare diffusione, le tecniche di intelligenza artificiale (cfr. il capitolo II, § 2).



Schema n. 2

A questo punto, le corrispondenze sono ordinate in base al grado di somiglianza con il dato iniziale: per questa ragione il riconoscimento non avviene mai con esattezza e il risultato è sempre subordinato ad una soglia variabile di errore (v. il capitolo I, § 2.5)[5]. Entro tale scenario, come già evidenziato in precedenza[6], l'impiego di tecniche di intelligenza artificiale costituisce un ulteriore livello di complessità per la presente ricerca, ma anche un passaggio ormai obbligato nell'analisi dell'impiego di processi automatizzati applicati al riconoscimento biometrico, dal momento che, il trattamento della rappresentazione digitalizzata di una *feature* senza l'applicazione di tali tecniche non può dirsi di per sé ormai particolarmente significativo. Per tale ragione, pur consapevoli dell'impiego ancora attuale - seppur ad oggi ormai poco diffuso - del dato biometrico che prescinda dall'utilizzo di procedimenti automatizzati per il raggiungimento di un *match*, il capitolo III prenderà in considerazione l'analisi dei soli *automated biometric recognition systems* (cfr. lo schema n. 2).

Orbene, come ormai noto, grazie all'impiego di queste tecniche computazionali, gli algoritmi alla base dei software sono costantemente "allenati" per trovare correlazioni tra le cd. *features* biometriche, a partire da sempre più ampi *datasets* (cfr. il capitolo I, § 3.3.1), acquisiti anche in condizioni non ottimali, a prescindere, quindi, da un intervento umano che "insegni" al sistema cosa sia quel determinato dato e come debbano essere distinte le singole parti che lo compongono[7]. In questo modo, i software individuano i cd. *patterns*, ossia schemi o sottoschemi presenti all'interno di dati non strutturati, utilizzati per allenare gli algoritmi, allo scopo di rintracciare le eventuali caratteristiche

[5] Cfr. E. Mordini, *Ethics and Policy of Forensic Biometrics*, in AA.VV., *Handbook of Biometrics for Forensic*, (a cura di) M. Tistarelli, C. Champod, Springer, Cham, 2017, pp. 357 e ss.
[6] Cfr. il capitolo II, §§ 1 e 4.
[7] Cfr. P. Viola, M. Jones, *Rapid Object Detection Using a Boosted Cascade of Simple Features*, in *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2001, pp. 511 e ss.

ricorrenti e determinare nuove correlazioni[8]. A tal proposito, come visto *supra*[9], le tecniche di IA permettono di instaurare delle associazioni fra i diversi schemi senza la necessità di essere espressamente programmati per tale funzione, ma solo attraverso l'analisi di esempi[10]. Comprendere e risalire all'architettura e al funzionamento di questi sistemi può risultare un'operazione estremamente complessa, se non addirittura impossibile[11], con evidenti potenziali ricadute su molteplici diritti fondamentali e garanzie processuali poste a presidio dell'individuo[12]. Invero, l'impiego di sistemi algoritmici come supporto per l'assunzione di decisioni e valutazioni aventi un impatto diretto sulla vita e sui diritti delle persone genera automaticamente l'esigenza di un controllo dei risultati che ne scaturiscono e una pretesa regolativa che il diritto è chiamato ad avanzare[13]. A tal proposito, quando queste tecniche automatiche di riconoscimento sono impiegate per finalità di prevenzione e repressione dei reati, si potrebbero porre delicati problemi di bilanciamento tra le esigenze di indagine penale e la tutela di alcune garanzie fondamentali[14]. Per vero, l'attenzione sarà qui concentrata unicamente sulla finalità di indagine e perseguimento dei reati[15]. Più nel dettaglio, per quel che interessa ai fini della presente ricerca, verrà analizzato *inter alia* il rapporto tra il dato biometrico digitalizzato impiegato nei sistemi automatici di riconoscimento e la garanzia della libertà personale, il *match* automatico fra due rappresentazioni digitali dello stesso tratto biometrico entro il

---

[8] Cfr. M. Van Otterlo, *A machine learning view on profiling*, in AA.VV., Privacy, *Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology*, (a cura di) M. Hildebrandt, K. De Vries, Routledge, Abingdon, 2013, p. 46, «*any methodology and set of techniques that can employ data to come up with novel patterns and knowledge, and generate models (e.g. profiles) that can be used for effective predictions about the data*».

[9] Cfr. il capitolo II, § 2.

[10] Cfr. M. A. Boden, *L'intelligenza artificiale*, Il mulino, Bologna, 2019, p. 82.

[11] cfr. il capitolo II, § 2.2.

[12] Cfr. FUNDAMENTAL RIGHTS AGENCY, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27.11.2019, reperibile all'indirizzo https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law (visualizzato in data 10.12.2021) e da ultimo ribadito da OECD, *OECD Framework For The Classification Of AI Systems*, n. 323/2022, reperibile all'indirizzo https://media-exp1.licdn.com/dms/document/C4E1FAQF_QAE4TIM42Q/feedshare-document-pdf-analyzed/0/1645957411385?e=1646474400&v=beta&t=RemFBR6_dzqS2FZn7xjyFszia8lSbsDyU5Gcv3tQIaI (visualizzato in data 4.3.2022).

[13] L'espressione "*policy before technology"* tratta da P. Dixon, *A Failure to "Do No Harm". India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S*., in *Health Technol.* 7, 2017, pp. 539–567 e richiamata nel titolo del presente capitolo, come un motto di protesta, evoca proprio tale esigenza.

[14] Cfr. il capitolo I, § 1.1 ove si presenta già la problematica. Sul tema cfr. *ex multis*, S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Springer, Cham, 2020, A. Zavrsnik, *Criminal justice, artificial intelligence systems and human rights*, in *ERA Forum* (2020), p. 575, C. Cesari, *L'impatto delle nuove tecnologie sulla giustizia penale - un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1174, A. Simoncini, *L'algoritmo incostituzionale:intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2019, p. 65, S. Marcolini, *Regole di esclusione e nuove tecnologie*, in *Criminalia* 1/2006, p. 391, L. Parlato, *Libertà della persona nell'uso delle tecnologie digitali*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*, Giuffrè, Milano, 2019, pp. 205 e ss., G. Di Paolo, *"Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione*, Cedam, Padova, 2008, pp. 1 e ss. e S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 6.

[15] La finalità di prevenzione dei reati sarà oggetto di una più estesa trattazione *infra*, nel capitolo IV, con riferimento alla modalità *real time* dei sistemi automatici di riconoscimento facciale (di questi s'è fatto cenno nel capitolo II, § 1.4.2).

canone del giusto processo e l'utilizzo di software automatici di riconoscimento a fronte del principio del *nemo tenetur se detegere*. Infine, saranno formulate alcune brevi riflessioni circa i potenziali rischi per la riservatezza dell'individuo derivanti dal recente sistematico impiego di alcuni software automatici di riconoscimento. Il rischio è che l'istanza securitaria di ricerca della verità, tramite la sistematica acquisizione di elementi di prova dal "corpo", trattati attraverso strumenti computazionali, possa "impoverire" le garanzie difensive.

Come emerge da queste prime considerazioni, siamo in presenza di un insieme variegato di questioni, saldamente connesse alla specifica tematica delle "prove scientifiche", la quale implica l'ottenimento di elementi conoscitivi acquisiti anche attraverso l'ausilio di criteri tecnico-scientifici, il cui indice di capacità dimostrativa rispetto all'accertamento del fatto di reato non può ancora darsi per scontato nel contesto culturale di riferimento, quantomeno rispetto al loro impiego in ambito giudiziario[16].

In seguito, dunque, alla presentazione delle caratteristiche fondamentali (v. il capitolo I) e delle analogie rispetto alla *digital evidence* (v. il capitolo II), questo capitolo affronterà l'analisi del dato biometrico entro i crismi classici della categoria processuale della "prova scientifica", considerando in particolare la capacità dimostrativa di un *match* scaturente da un software automatico di riconoscimento rispetto ai fatti oggetto di prova, per poi passare alla trattazione dell'impiego dello stesso nello spettro delle garanzie fondamentali poste a tutela dell'indagato.

Prima di addentrarsi in uno studio approfondito del rapporto trilaterale fra dato biometrico digitalizzato (nelle diverse estrinsecazioni considerate nella presente ricerca), *digital evidence* e prova scientifica, si ritiene opportuno fornire una ricostruzione esegetica completa, seppur non esaustiva, del legame - da sempre molto ravvicinato - tra prova, scienza e processo penale.

1.1 Prova, scienza e processo penale: un trinomio in continua evoluzione

Il tema della prova scientifica e del suo ruolo nella formazione del convincimento giudiziale costituisce «un complesso fenomeno, articolato e diversificato in molteplici forme di manifestazione»[17]. Per lungo tempo e non solo in Italia, si è discusso intorno ai rapporti tra scienza e

[16] Cfr. P. Rivello, *Tecniche scientifiche e processo penale*, in *Cass. pen*., Fasc. 4, 2013, p. 1691 e ss.

[17] Cfr. O. Dominioni, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2005, p. 12. Sul tema, senza alcuna pretesa di esaustività, cfr. E. Amodio, *Perizia e consulenza tecnica nel quadro probatorio del nuovo processo penale*, in *Cass. pen*., 1989, p. 1970, E. Amodio, *Libero convincimento e tassatività dei mezzi di prova: un approccio comparativo*, in *Riv. it. dir. proc. pen*., 1999, pp. 3 e ss., S. Jasanoff, *La scienza davanti ai giudici. La regolazione giuridica della scienza in America*, Giuffrè, Milano, 2001, G. Canzio, *Prova scientifica, ragionamento probatorio e libero convincimento del giudice nel processo penale*, in *Diritto penale e processo*, 2003, pp. 1193 e ss., F. Stella, *Leggi scientifiche e spiegazione causale nel diritto penale*, 2° ed., Milano, 2000, p. 156, P. Tonini, *Prova scientifica e contraddittorio*, in *Diritto penale e processo*, 2003, pp. 1459 e ss., C. Conti, *Evoluzione della scienza e ruolo degli esperti nel*

diritto[18]. Mirjan Damaska scriveva, alcuni anni or sono, che guardare al futuro del processo penale «significa soprattutto parlare della progressiva adozione di modelli scientifici nell'indagine sui fatti», perché «un numero sempre più elevato di fatti rilevanti nel processo [può ormai essere dimostrato] soltanto con strumenti tecnici sofisticati»[19]. Invero, la relazione intercorrente tra conoscenza giudiziaria e conoscenza scientifica risulta alquanto risalente, se si considera che uno degli scritti di riferimento - il saggio "*Scientificità della prova e libera valutazione del giudice*" di Vittorio Denti – risulta datato 1972[20]. Al proposito, l'Autore formulava alcune riflessioni di estrema attualità con cui preannunciava il dibattito odierno e ne enunciava, sotto alcuni aspetti, le conclusioni, sostenendo che «i metodi scientifici non possono offrire nuove categorie di prove, ma possono servire ad una migliore ricerca della verità». Già veniva delineato uno dei nodi salienti della problematica relativa ai rapporti tra scienza e processo, quello avente ad oggetto la classificazione della prova cd. "scientifica" entro il catalogo tipizzato dal legislatore. Essa è individuabile ogni volta che l'accertamento dei fatti richieda nozioni e tecniche che travalicano il sapere dell'uomo medio - e del giurista - e non siano riconducibili

processo penale, in AA.VV., *Medicina e diritto penale*, (a cura di) S. Canestrari, F. Giunta, R. Guerrini, T. Padovani, *STUDI discipline penalistiche Criminalia*, Napoli, 2009, pp. 335-358, G. Ubertis, *La prova scientifica e la nottola di Minerva*, in AA.VV., *La prova scientifica nel processo penale*, (a cura di) L. De Cataldo Neuburger, Cedam, Padova, 2007, p. 83, M. Daniele, *Prova scientifica e regole di esclusione*, in AA.VV., *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Luparia, Wolters Kluwer, Milano, 2017, pp. 489 e ss., P. Felicioni, *Processo penale e prova scientifica: verso un modello integrato di conoscenza giudiziale*, in *Cass. pen*., 2013, pp. 1620 e ss., M. Taruffo, *La prova dei fatti giuridici. Nozioni generali*, Giuffrè, Milano, 1992, M. Taruffo, *L'uso probatorio della scienza nel processo*, in AA.VV., *L'uso della prova scientifica nel processo penale*, (a cura di) G. Cucci, M. Gennari, A. Gentilomo, Rimini, 2012, pp. 45 e ss., P. Tonini, *La Cassazione accoglie i criteri Daubert sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza*, in *Dir. pen. Cont*., 2011, pp. 1341 e ss., L. D'Auria, *Prova penale scientifica e giusto processo*, in *Giust. pen.* 2004, p. 22, G. Canzio, *La motivazione della sentenza e la prova scientifica:* "*reasoning by probabilities*", in AA.VV., *Scienza, diritto e processo penale nell'era del rischio*, (a cura di) A. Amato, G. Flora, C. Valbonesi, 2019, Giappichelli, Torino, p. 50, G. Tuzet, *L'algoritmo come pastore del giudice? Diritto, tecnologie, prova scientifica*, in *MediaLaws*, 2019, p. 4, S. Renzetti, *La prova scientifica nel processo penale: problemi e prospettive*, in *Rivista di Diritto Processuale*, 2/2015. E' "scientifica" quella prova che: «partendo da un fatto dimostrato, utilizza una legge scientifica per accertare un fatto "ignoto" per il giudice. Ha tale caratteristica quella legge che è stata ricavata in modo "scientifico", e cioè con un metodo sperimentato mediante l'individuazione del tasso di errore e sottoposto alla critica della comunità degli esperti». P. Tonini, *Prova scientifica e contraddittorio*, cit., p. 1459. G. Di Paolo, *"Tecnologie del controllo" e prova penale.*, cit., p. 8, sottolinea come entro la locuzione "prova tecnico-scientifica" possa essere ricondotta una molteplicità di fenomeni assai diversi tra loro, come per esempio «la ricerca della prova nella fase investigativa attraverso le cd. tecnologie del controllo; l'introduzione della prova nel processo attraverso l'impiego di mezzi tecnologici sofisticati; il formarsi della prova (qui intesa come risultato) attraverso un giudizio di inferenza probatoria che rende necessario integrare il patrimonio conoscitivo dell'organo giudicante con conoscenze specialistiche pertinenti al mondo della scienza e della tecnica (…)».

[18] «(…) la scienza ha costretto i giuristi a confrontarsi con problemi e con saperi nuovi; il diritto vivente, in modo più o meno consapevole, va delineando inediti paradigmi o, quanto meno, sottopone paradigmi antichi a letture innovative per renderli compatibili con contenuti inusitati, portando all'interno delle consolidate (e talora risalenti) architetture un'aria così fresca e vigorosa da togliere, sulle prime, il respiro». C. Conti, *Scienza controversa e processo penale: la Cassazione e il "discorso sul metodo"*, in *Dir. Pen. e Processo, 2019, 6*, 848. Cfr. anche T. Alesci, *Corpo dell'imputato (fonte di prova nel processo penale)*, in *Digesto delle Discipline Penalistiche*, Utet, Milano, 2018, p. 80.

[19] Cfr. M. Damaska, *Il diritto delle prove alla deriva*, Il Mulino, Bologna, 2003, p. 205.

[20] Cfr. Denti, *Scientificità della prova e libera valutazione del giudice*, in *Riv. dir. proc*., 1972.

nell'alveo delle massime di esperienza[21]. Come più volte evidenziato dalla dottrina, sarebbe tuttavia più corretto esprimersi in termini di "prove scientifiche" rispetto a una categoria unitaria, in quanto «ogni scienza ha i suoi paradigmi, i suoi concetti generali, i suoi criteri di validità: dunque, nel processo non entra un solo tipo di scienza e un solo tipo di verità scientifica»[22].

Il sistema italiano ha riconosciuto la legittimazione alla prova scientifica con un certo ritardo[23]: la celebre "sentenza Franzese" della Corte di cassazione del 2002 ha rappresentato l'"anello di congiunzione" tra «la nuova concezione di scienza, i modi del conoscere giudiziale e le dinamiche e i contenuti dell'onere della prova»[24], ponendo le basi per la codificazione del principio dell'oltre ogni ragionevole dubbio mediante un'integrazione dell'art. 533 c.p.p. con la legge 46 del 2006[25].

Nel nuovo vigore attribuito al dibattito sul rapporto fra procedimento probatorio penale e il metodo scientifico di accertamento dei fatti, rinnovato dalla progressiva irruzione di tecniche ad alto contenuto tecnologico nel campo forense, la riflessione di Denti sembra conservare immutata la sua modernità[26]. È, quindi, ormai indiscutibile che la prova scientifica sia sempre più destinata a ricoprire un ruolo di straordinario rilievo nel ragionamento e nella decisione del giudice, ponendosi come strumento idoneo anche per la ricostruzione del nesso causale e il raggiungimento della verità processuale[27]. In

---

[21] Consistenti «nei principi di scienza teorica, nei metodi della scienza applicata, nelle tecnologie e apparecchiature con cui questi corpi di scienza vengono applicati per la ricostruzione processuale del fatto». O. Dominioni, *In tema di nuova prova scientifica*, in *Dir. pen. proc*., 2001, p. 1061.

[22] «Esse derivano dal mondo indefinito e costantemente mutevole degli studi che scienza teorica, scienza applicata e tecnologia conducono, delle pratiche specialistiche che registrano con l'esperienza l'andamento di dati fenomeni: con risultati, in tutti questi campi, mai definitivi e irreversibili (…)». O. Dominioni, *La prova penale scientifica*, cit., pp. 26 e ss. Cfr. anche M. Bargis, *Note in tema di prova scientifica nel processo penale*, in *Riv. Dir. Proc*., 2011, 1, p. 47 e F. Caprioli, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen*., 2003, p. 3523.

[23] Cfr. T. Alesci, *Il corpo umano fonte di prova*, Wolters Kluwer, Milano, 2017, p. 36 ove si sostiene che il passaggio dal positivismo scientifico al neopositivismo, accolto nel sistema angloamericano in seguito alla sentenza Daubert, pronunciata dalla Corte Suprema degli Stati Uniti nel 1993 è avvenuto con ritardo (*Daubert v. Merrel Dow Pharmaceuticals, Inc*., 509 U.S., 579, 113, trad. in *Riv. Trim. Dir. proc. civ*., 1996, p. 278).

[24] Cfr. P. Tonini, *L'influenza della sentenza Franzese sul volto attuale del processo penale*, *Dir. pen. proc*., 2012, pp. 1225 e ss.; si veda Cass., sez. I, 11.9.2002, Franzese, in *Riv. it. dir. proc. pen*., 2002, p. 1133. Nella motivazione si afferma che la corretta ricostruzione scientifica da accogliere è quella che «resiste all'urto del contraddittorio tra gli esperti». In estrema sintesi, è possibile affermare che fino alla metà del secolo scorso è stata accolta una concezione positivistica della scienza. In base a tale filosofia, la scienza è illimitata, completa e infallibile. Dagli anni '40 del secolo scorso, si è cominciata ad erodere tale idea inaugurando la concezione post-positivistica per la quale la scienza è limitata, incompleta e fallibile. Cfr. P. Tonini, *Progresso tecnologico, prova scientifica e contraddittorio*, in AA.VV., *La prova scientifica nel processo penale*, (a cura di) L. De Cataldo Neuburger, Cedam, Padova, 2007, p. 58 e cfr. P. Tonini, *Prova scientifica e contraddittorio*, in *Diritto penale e processo*, 2003, pp. 1459 e ss.

[25] Cfr. P. Felicioni, *Processo penale e prova scientifica: verso un modello integrato di conoscenza giudiziale*, in *Cass. pen*., fasc. 4, 2013, p. 1620 ove l'Autrice afferma che «tale pronuncia ha rappresentato l'anello di congiunzione tra "la nuova concezione di scienza, i modi del conoscere giudiziale e le dinamiche e i contenuti dell'onere della prova", spianando la via alla codificazione della regola dell'oltre ragionevole dubbio mediante un'integrazione dell'art. 533 c.p.p. con legge n. 46 del 2006». Cfr. su questo punto anche C. Conti, *Al di là del ragionevole dubbio*, in AA.VV., *Novità su impugnazioni penali e regole di giudizio*, (a cura di) A Scalfati, Ipsoa, 2006, p. 91.

[26] Peraltro, «(…) l'incremento esponenziale dei risultati della ricerca scientifica pare indurre il timore che il diritto non sia in grado di abbracciarne tutti gli sviluppi». G. Ubertis, *La prova scientifica e la nottola di Minerva*, cit., p. 84.

[27] M. Bargis, *Note in tema di prova scientifica nel processo penale*, in *Riv. Dir. Proc.*, 2011, 1, p. 47, G. Canzio, *La motivazione della sentenza e la prova scientifica:* "*reasoning by probabilities*", in AA.VV., *Prova scientifica e processo penale*, (a cura di) G.

particolare, la società sta attraversando, a livello globale, un periodo di sviluppo inedito e rapidissimo sul piano dell'elaborazione e dell'impiego di strumenti tecnologici innovativi ed avanzati, in tutti i campi della vita individuale e collettiva[28]. Peraltro, è possibile constatare come scienza e processo corrano a differenti velocità[29]: non sempre, infatti, il legislatore è in grado di fronteggiare a livello normativo le sfide che l'evoluzione tecnologica gli pone[30]. Tale cronico ritardo si riflette nella prassi, alimentando interpretazioni giurisprudenziali che hanno ad oggetto sempre più di frequente nuove e inedite forme di prove scientifiche. Invero, il metodo del contraddittorio impone la costante verifica e falsificazione dell'affidabilità della prova scientifica[31], coerentemente con l'insegnamento di Karl Popper[32]. Ed è sulla base dei continui severi controlli e tentativi di falsificazione che si può giungere

Canzio, L. Luparia, Wolters Kluwer, Milano, 2017, pp. 9 e ss., O. Dominioni, *La prova penale scientifica*, Giuffrè, Milano, 2005, M. Taruffo, *La prova scientifica nel processo civile*, in *Riv. trim. dir. proc. civ*., 2005, p. 1079, F. Caprioli, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen*., 2008, p. 3520, G. Canzio, *Prova scientifica, ricerca della verità e decisione giudiziaria nel processo penale*, in AA.VV., *Scienza e casualità*, (a cura di) C. Di Maglie, S. Seminara, Cedam, Padova, 2006, p. 143, C. Conti, *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, Giuffrè, Milano, 2011, p. 61, S. Lorusso, *La prova scientifica*, in AA.VV., *La prova penale*, (a cura di) A. Gaito, vol. II, Utet, Torino, 2008, G. Ubertis, Il giudice, la scienza e la prova, in *Cass. pen*. 2011, pp. 4111 e ss. M. Torre, *Privacy e indagini penali*, Giuffrè, Milano, 2020, pp. 2 e ss.

[28] Per tale ragione, nel novero degli strumenti scientifico-tecnici, la dottrina distingue necessariamente fra quelli che sono già oggetto di un'esperienza consolidata e condivisa nell'uso giudiziario e quelli "nuovi o controversi e di elevata specializzazione". Dominioni rileva che anche gli strumenti tecnico-scientifici consueti, come ad esempio, la rilevazione e l'analisi delle impronte digitali possono vedersi sopraggiungere da nuove formulazioni che li pongono in discussione, fino a renderli ad un certo punto problematici. O. Dominioni, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, cit., p. 13 e F. Caprioli, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, cit., p. 3523.

[29] Inoltre, è bene tenere a mente come scienza e processo penale appartengano a mondi completamente differenti: il processo penale non può chiedere alla scienza più di quanto questa possa fornire, anche se da sempre l'uomo ha scaricato le sue esigenze di sapere sulla stessa. Com'è stato affermato da P. Tonini, *Progresso tecnologico, prova scientifica e contraddittorio*, in AA.VV., *La prova scientifica nel processo penale*, (a cura di) L. De Cataldo Neuburger, Cedam, Padova, 2007, p. 54: «nel mondo dell'"essere" lo scienziato può ricavare le regole dell'accadere dei fatti, e cioè i collegamenti causa-effetto: si tratta delle leggi scientifiche. Viceversa, la legge penale fa parte del "dover essere", e cioè dei doveri». Sul ritardo del diritto rispetto al progredire scientifico cfr. G. Ubertis, *La prova scientifica e la nottola di Minerva*, cit., pp. 84-85, S. Marcolini, *Regole di esclusione e nuove tecnologie*, in *Criminalia*, 2007, p. 395 e O. Dominioni, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, p. 7 ove in *Premessa*, l'autore afferma: «la cultura della conoscenza giudiziaria ha registrato e, in misura non irrilevante, sta ancora registrando un sensibile ritardo nel farsi carico del rinnovamento delle concezioni epistemologiche in ambito scientifico e tecnologico. Ma ancora maggiore è il ritardo nel mettere a punto i congegni processuali mediante i quali tali concezioni e le nuove risorse scientifico-tecniche di conoscenza siano praticabili nella funzione probatoria con la necessaria affidabilità».

[30] Cfr. T. Alesci, *Il corpo umano come fonte di prova*, Wolters Kluwer, Milano, 2017, p. 37.

[31] Sulle caratteristiche delle leggi scientifiche cfr. G. Ubertis, *La prova penale. Profili giuridici ed epistemologici*, Giappichelli, Torino, 1995, p. 33, P. Tonini, *La prova penale*, Cedam, Padova, 2000, p. 38. Il principio del contraddittorio costituisce un vero e proprio "canone orientativo" della giurisdizione penale, cfr. A. Cabiale, *I limiti alla prova nella procedura penale europea*, Wolters Kluwer, Milano, 2019, p. 1, G. Giostra, *Analisi e prospettive di un modello incompiuto*, in *Quest. Giust*., 2001, p. 1130.

[32] Cfr. K. Popper, *The poverty of the historicism* (1944-1945), (trad. it.) S. Veca, *Miseria dello storicismo*, Feltrinelli, Milano, 1997, p. 120: «la scoperta di esempi che convalidano una teoria vale pochissimo se non abbiamo tentato, senza riuscirvi, di trovare degli esempi che la confutano. Perché, se abbiamo poco senso critico, troveremo sempre quello che desideriamo: cercheremo e troveremo delle conferme; distoglieremo lo sguardo da ciò (e quindi non lo vedremo) che potrebbe mettere in pericolo le teorie che ci sono care. In questo modo è facilissimo ottenere prove, apparentemente schiaccianti di un teoria che, se fosse stata invece avvicinata con animo critico, sarebbe confutata».

ad un giudizio di affidabilità della teoria[33]. Se quest'ultima risulta in grado di resistere a diversi tentativi di falsificazione può dirsi verificata e può essere accolta. Il principale pregio di tale riflessione è quello di aver sostituito ad un'idea assoluta del sapere il principio secondo cui «propriamente scientifico è ciò che distrugge la scienza precedente»[34]. Ne consegue che la conoscenza è "scientifica" se, in seguito a falsificazione, risulta possibile individuare il suo preciso funzionamento e il relativo tasso di errore. Le eventuali confutazioni e la falsificazione delle teorie rappresentano in tal modo la trasposizione del contradditorio processuale nella scienza. Orbene, le peculiarità delle argomentazioni processuali possono essere preservate solo se si tiene a mente che la scienza è fallibile, «una disputa ininterrotta che ha mandato in frantumi una serie sconfinata di teorie»[35].

Proprio nell'ambito della giustizia penale, il sapere scientifico ritrova un incentivo per un suo costante progresso. Quest'ultimo deve avvenire, però, assicurando il completo rispetto delle garanzie inviolabili delle parti. Lo studio del complesso rapporto fra scienza e processo penale deve essere condotto, da un lato, tenendo a mente l'influenza delle prove scientifiche sul ragionamento condotto dal giudice, dall'altro, analizzando la natura dello strumento utilizzato nella circostanza concreta[36]. Sotto il primo profilo, si è assistito nel tempo ad una riduzione del margine di valutazione operabile dal giudice: non appena le conoscenze impiegate nel processo superino quelle detenute dall'uomo medio, si assiste ad un progressivo svuotamento delle necessarie competenze valutative in capo all'organo giudicante[37]. La soluzione a tale deriva è rappresentata dall'inserimento nel ragionamento giudiziale di criteri predefiniti, allo scopo di ammettere solo teorie e metodi ritenuti affidabili ed escludere la cd. "*junk science*"[38]. Invero, nel 2010, sono state poste le basi per un ulteriore mutamento

---

[33] Si tenga presente che, in ogni caso, il falsificazionismo non è universalmente accettato dai filosofi della scienza. Tra i postpopperiani, fondamentale è stato l'approccio di P. Feyerabend, *Against Method. Outline of an Anarchistic Theory of Knowledge* (1975), (trad. it.) L. Sosio, *Contro il metodo. Abbozzo di una teoria anarchica della conoscenza*, Milano, 1979. Ad avviso dello studioso, il falsificazionismo deve essere superato da una concezione basata sul fatto che non si può rifiutare a priori nessun metodo: proprio l'apertura ha consentito in passato lo sviluppo della scienza.

[34] Cfr. P. Ferrua, *Presentazione*, in AA.VV, *La prova scientifica nel processo penale*, (a cura di) G. Carlizzi, G. Tuzet, Giappichelli, Torino, 2018, p. 11.

[35] Cfr. K. Popper, *Logik der Forschung, Wien*, 1935, (trad. it.) M. Trinchero, *Logica della scoperta scientifica*, Torino, 1970, p. 22. Si veda anche P. Ferrua, *Presentazione*, cit., p. 13, ove sostiene che la prova "oltre ogni ragionevole dubbio" non è dissimile dalla resistenza ai tentativi di falsificazione: «nel processo la falsificazione dell'accusa non si realizza soltanto in forma positiva per la presenza di fatti incompatibili con la colpevolezza, documentati per lo più dalle prove a difesa, ma anche in forma negativa per la mancata o insufficiente prova dei fatti che dovrebbero discendere dall'ipotesi accusatoria e, come tali, rappresentare il complesso delle prove a carico; dunque, se correttamente intese, prova "oltre ogni ragionevole dubbio" e resistenza alla falsificazione esprimono in sostanza concetti equivalenti». Su questi temi, si veda anche P. Tonini, *Prova scientifica e contradditorio*, in *Dir. pen. e proc*., 2003, p. 1459.

[36] Cfr. M. Bargis, *op. cit*., p. 47.

[37] Cfr. M. Bargis, *op. cit*., p. 47.

[38] «La scienza spazzatura è l'immagine speculare della vera scienza, con molto della stessa forma, ma niente della stessa sostanza». Cfr. P. W. Huber, *Galileo's revenge. Junk science in the Courtroom*, Basic books, New York, 1993, pp. 2, 40 e 92, ove l'Autore ha cercato di sottolineare criticamente le difficoltà incontrate dal mondo del diritto nel distinguere la scienza minoritaria dalle mistificazioni pseudo-scientifiche. Sul punto si veda anche F. Centonze, *Scienza spazzatura e scienza corrotta nelle attestazioni e valutazioni dei consulenti tecnici nel processo penale*, in *Riv. it. dir. proc. pen.*, 2001, pp. 1234 e ss., D.E. Bernstein, *Junk Science*

di regime[39]: con la sentenza Cozzini[40], come noto, sono stati interamente accolti nel panorama giuridico italiano i criteri elaborati dalla giurisprudenza statunitense[41], concependo in modo del tutto

in the United States and the Commonwealth, in *Yale J. Int. L.*, 1996, p. 123, M. Bargis, *Note in tema di prova scientifica nel processo penale*, in *Riv. D. Proc*., 2011, pp. 47 e ss., C. Conti, *Il processo si apre alla scienza. Considerazioni sul procedimento probatorio e sul giudizio di revisione*, in *Riv. It. Dir. Proc. Pen.*, 2010, pp. 1204 e ss., F. Caprioli, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen*., 2009, pp. 380 e ss.

[39] Dal 2002 al 2010, la Corte di cassazione ha eseguito un percorso ermeneutico rispetto ai criteri delineati dalla giurisprudenza statunitense, si veda in proposito: Cass. pen., Sez. I, 21.5.2008, n. 31456 in *CED Cass* n. 240764, Franzoni, in tema di applicazione della *Bloodstain Pattern Analysis* - tipo di indagine che studia la morfologia e la 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 statunitense.

[40] Cass. pen., Sez. IV, 17.9.2010, n. 43786 in *CED Cass* n. 248944: «per valutare l'attendibilità di una teoria occorre esaminare gli studi che la sorreggono. Le basi fattuali sui quali essi sono condotti. L'ampiezza, la rigorosità, l'oggettività della ricerca. Il grado di sostegno che i fatti accordano alla tesi. La discussione critica che ha accompagnato l'elaborazione dello studio, focalizzata sia sui fatti che mettono in discussione l'ipotesi sia sulle diverse opinioni che nel corso della discussione si sono formate. L'attitudine esplicativa dell'elaborazione teorica. Ancora, rileva il grado di consenso che la tesi raccoglie nella comunità scientifica. Infine, dal punto di vista del giudice, che risolve casi ed esamina conflitti aspri, è di preminente rilievo l'identità, l'autorità indiscussa, l'indipendenza del soggetto che gestisce la ricerca, le finalità per le quali si muove».

[41] Cfr. D. L. Faigman, E. Porter, M. J. Sacks, *Cheek your Cristal Ball at the Courthouse Door, Please: Exploring the Past, Understanding the Present, and Worrying about the Future of Scientific Evidence*, in 15 *Cardozo L. Rev.* 1803 (1994). I pilastri dell'orientamento giurisprudenziale statunitense in materia sono costituiti dai due *leading cases*. Innanzitutto il caso *Frye vs. United States* (*Frye v. Unites States*, 293 F. 1013, D.C. Cir., 1923), deciso dalla Corte d'appello del distretto di Columbia e, in secondo luogo, la decisione *Daubert vs. Merrel Dow Pharmaceuticals* (*Daubert v. Merrell Dow Pharmaceuticals*, 509, U.S. 579 (1993), pubblicata nel 1993 dalla Suprema Corte Federale. Di tale decisione si può vedere la traduzione non integrale a cura di A. Dondi, in *Riv. dir. proc. civ*., 1996, pp. 277 e ss., nonché in F. Stella, *Leggi scientifiche e spiegazione causale nel diritto penale*, Giuffrè, Milano, 2000, pp. 424 e ss. 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. Tuttavia, tale criterio interpretativo non ha tardato 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 (cfr. B. Burack, *Analisi critica della teoria, del metodo e delle limitazioni del "lie detector"* (1955), trad. ital. Di G. Bellavista, in *Riv. dir. proc. pen*., 1956, pp. 199 e ss.; con riferimento alla questione dell'ammissibilità della prova poligrafica, si veda D. Gallai, *Poligraph Evidence in Federal Courts: Should it be admissible*, in 36 *Am. Crim. L. rev*., 88 (1999)). 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 posta 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 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 (*fit*); 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 scientific testimony*, può comunque offrire conferme importanti in ordine alla validità di una teoria o tecnica scientifica che si intenda utilizzare nel processo. Questi standard, sono stati poi espressamente regolamentati nella *Rule* 702 delle "*Federal Rules of Evidence*" (2011), come segue: 1) la prova peritale è il prodotto del metodo scientifico, empiricamente resistente alla prova contraria; 2) l'apporto metodologico deve esser revisionato da esperti diversi e pubblicato; 3) il margine di

innovativo il ruolo dell'organo giudicante innanzi al sapere specialistico[42]. A tal proposito, il giudice «non può certamente assumere un ruolo passivo di fronte allo scenario del sapere scientifico»[43], ma neppure pretendere di avere sufficienti «conoscenze e (…) competenze per esperire un'indagine [solitaria su quello scenario]»[44]. Egli deve piuttosto confrontarsi con gli esperti condotti davanti a lui, cioè operare come «garante della scientificità della conoscenza fattuale espressa dal processo» e «svolgere un penetrante (…) ruolo critico, divenendo (…) custode del metodo scientifico»[45]. L'idea è quella di una vera e propria "cultura dei criteri", funzionale al controllo sull'operato degli esperti anche in assenza di una previsione normativa, che sia desumibile dalla letteratura giuridica e che guidi il giudice in sede di valutazione della prova[46]. Infatti, «il giudice non ha bisogno di possedere tutte le nozioni e le tecniche che occorrono allo scienziato per porre in essere la prova dovendo egli piuttosto disporre di schemi razionali che gli consentano di stabilire il valore della prova scientifica ai fini dell'accertamento del fatto. Anche sotto questo profilo non si tratta di identità di metodi tra il giudice

errore è necessariamente conoscibile; 4) la tecnica è costantemente monitorata, in termini di rispondenza a parametri standard; 5) la tecnica e il relativo apporto metodologico sono avallati dalla comunità scientifica. Per una ricostruzione approfondita si veda O. Dominioni, *La prova penale scientifica*, cit., pp. 113 e ss. e G. Carlizzi, *La valutazione della prova scientifica*, Giuffrè, Milano, pp. 89 e ss.

[42] 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.

[43] Cfr. Cass. pen., Sez. IV, 17.9.2010, n. 43786, cit., p. 40.

[44] Cfr. Cass. pen., Sez. IV, 17.9.2010, n. 43786, cit., p. 45.

[45] Cfr. Cass. pen., Sez. IV, 17.9.2010, n. 43786, cit., p. 40. Per un approfondimento sulla sentenza Cozzini, cfr. D. Pulitanò, *Difesa penale e saperi sul mondo*, in AA.VV., *La prova scientifica nel processo penale*, (a cura di) G. Carlizzi, G. Tuzet, Giappichelli, Torino, 2018, p. 54 e G. Carlizzi, *Giudice 2.0 e uso del sapere specialistico nel processo penale*, in *Processo penale e giustizia* n. 4/2017, p. 746. L'interpretazione adottata dalla sentenza Cozzini è stata accolta anche da successive pronunce giurisprudenziali: si veda Cass. pen., Sez. II, 8.3.2011, n. 12751 in *CED Cass* n. 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. Analogamente Cass. pen., Sez. VI, 4.7.2013, n. 34531 in *CED Cass* n. 256136, 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 di affidabilità ai risultati della nuova indagine. Infine, Cass. pen., Sez. V, 27.3.2015, n. 36080 in *CED Cass* n. 264860 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». Sul punto si veda anche la pronuncia del procedimento per i fatti relativi alla morte di Yara Gambirasio, Cass. pen., sez. I, 23.11.2018, n. 52872 in *CED Cass* n. 275058: «(…) il criterio da adottare per valutare se una certa disciplina possa reputarsi scientifica, e quindi affidabile, è quello della sua controllabilità o falsificabilità empirica. Il controllo del giudice non può quindi limitarsi alla sola circostanza se l'esperto sia stato più o meno diligente, me deve verificare se la tesi prospettata risulti convincente o fondata. A tal fine s'impone un'attenta verifica delle garanzie di competenza e imparzialità che offre l'esperto, per evitare che l'accertamento della verità sia affidato alla "scienza spazzatura" o alla "frode scientifica"». Il giudice è, dunque, «il garante dell'affidabilità del sapere scientifico riversato nel processo e di colui che a tale operazione di riversamento provvede, cioè l'esperto». Su questo punto cfr. anche C. Conti, *Scienza controversa e processo penale: la Cassazione e il "discorso sul metodo"*, in *Dir. pen. e processo*, 2019, 6, p. 848.

[46] «Spetta allo stesso giudice enucleare questi criteri, che può attingere dall'elaborazione giurisprudenziale, dalla letteratura giuridica, dalla *Forensic Science*, dallo stesso ambito scientifico posto che gli studiosi, nel definire un nuovo principio scientifico o un nuovo metodo tecnologico, intanto ne accreditano la validità in quanto mettono a punto anche gli indici della loro verifica». O. Dominioni, *La prova penale scientifica.*, cit. p. 71. Sul punto cfr. anche P. Tonini, *Progresso tecnologico, prova scientifica e contraddittorio*, cit., p. 74.

e lo scienziato, ma dell'impiego da parte del giudice di strumenti di analisi che permettano la valutazione di prove prodotte con metodi scientifici»[47]. Proprio con riferimento a ciò, si ritiene utile fare brevemente cenno ad alcune delle *quaestiones* che troveranno maggiore approfondimento, nei successivi paragrafi. La prima serie di domande concerne il ruolo processuale di un *match* scaturente da un software automatico di riconoscimento: a quale categoria di prova risulta ragionevole ricondurlo? In mancanza di una espressa regolamentazione legislativa, il giudice ammetterà questo peculiare elemento di prova?

La seconda serie di *quaestiones,* strettamente connesse alla prima, concerne invece l'attendibilità del risultato e il suo significato intrinseco rispetto all'accertamento dei fatti oggetto di prova.

1.1.1 Il ruolo di un *automated biometric match* per l'accertamento del fatto di reato

Per l'analisi di tale argomento occorre indagare quale sia l'effettiva capacità dimostrativa, o meglio il valore probatorio di un risultato, espresso in termini probabilistici, derivante dall'utilizzo di un software automatico di riconoscimento rispetto all'oggetto di prova, così come descritto dall'art. 187 c.p.p.[48]. In altre parole, ciò su cui si ritiene necessario soffermarsi è l'effettiva funzione informazionale di un *match* e il suo contributo conoscitivo per assicurare l'accertamento dei fatti di cui si dibatte nel procedimento. L'obiettivo del processo penale, come noto, è «l'accertamento del fatto di reato attraverso la ricostruzione dell'evento, per tale ricostruzione il giudice si avvale del procedimento probatorio che ha come obiettivo anelato la "conquista" della verità, per lo meno di quella abitualmente definita "verità processuale"»[49]. Trattasi, infatti, dell'accertamento processuale che non può coincidere con la ricerca di una "verità assoluta" dal momento che risulta sempre ravvisabile, per quanto limitato, un inevitabile margine di incertezza[50]. In tal senso, la prova rappresenta il veicolo attraverso il quale il processo può raggiungere il suo scopo, costituendo il fondamento della decisione giudiziale. Entro tale contesto, vale la pena domandarsi dunque che cosa

[47] Cfr. M. Taruffo, *La prova dei fatti giuridici*, Giuffrè, Milano, 1992, p. 308.

[48] *Ex* art. 187 c.p.p., oggetto di prova sono i fatti che si riferiscono all'imputazione, alla punibilità e alla determinazione della pena e della misura di sicurezza, oltre ai fatti dai quali dipende l'applicazione di norme processuali e quelle aventi ad oggetto la responsabilità civile derivante da reato, se vi è costituzione di parte civile. Come noto, le prove individuate in base a quanto stabilito dall'art. 187 c.p.p. per essere ammesse non devono essere vietate dalla legge, manifestamente superflue o irrilevanti (art. 190 c. 1 c.p.p.). Per un approfondimento cfr. G. Ubertis, *La conoscenza del fatto nel processo penale*, Giuffrè, Milano, 1992, p. 17 e M. Nobili, *Il "diritto delle prove" ed un rinnovato concetto di prova*, in AA.VV., *Commento al nuovo codice di procedura penale*, (a cura di) M. Chiavario, Utet, Torino, II, 1990.

[49] Cfr. L. Saponaro, *L'impatto processuale delle immagini: fotografie e videoriprese*, Wolters Kluwer, Milano, 2020, p. 19. Sul tema cfr. A. Melchionda, voce *"Prova in generale (dir. proc. pen.)"*, in *Enc. Dir*. XXXVIII, Torino, 1988, p. 843 e L. P. Comoglio, *Prove e accertamento dei fatti nel nuovo codice di procedura penale*, in *Riv. It. Dir. pen*., 1990, p. 113.

[50] Per un approfondimento cfr. F. Caprioli, *Verità e giustificazione nel processo penale*, in *Revista Brasileira de Direito Processual Penal*, vol. 3, n. 1, 2017.

rappresenti un *match*, scaturente da un software automatico di riconoscimento, rispetto ai fatti oggetto di prova.

Punto di partenza per l'analisi della *quaestio* è costituito allora dalla definizione di "prova". In assenza di una definizione normativa essa può essere intesa ragionevolmente come «ciò che si assume come dimostrazione di un accadimento e/o di sue determinate modalità», ovvero come «mezzo di cui ci si serve per ottenere quella dimostrazione»[51]. In tal senso, il *genus* prova è costituito da due *species*, intese sia come "strumento di conoscenza" sia come "risultato gnoseologico"[52]. Nel primo caso, il riferimento è alla vera e propria fase di formazione della prova (richiesta, ammissione, assunzione). Nel secondo, essa rappresenta la soluzione cognitiva e ha ad oggetto il momento valutativo della stessa. A tal proposito, l'*iter* conoscitivo compiuto dal giudice presenta una struttura di tipo inferenziale: il fatto storico di reato viene ricostruito dal giudice attraverso i risultati delle prove acquisite nel processo[53].

Orbene, proprio con riferimento alla delimitazione del concetto di prova e al procedimento gnoseologico giudiziale, va richiamata – tra le numerose classificazioni del fenomeno probatorio – la distinzione fra prova "diretta", con la quale s'intende quella in cui tra la proposizione probatoria e la proposizione da provare non si interpongono proposizioni intermedie, e la prova "indiretta", in cui invece sono presenti proposizioni interposte fra l'oggetto di prova e un determinato fatto noto[54]. In altre parole, l'elemento distintivo fra le due categorie di prova concerne essenzialmente la diretta riferibilità o meno al *thema probandum* principale, quale risulta dall'art. 187 c.p.p.[55]. Come noto, le prove appartenenti a questa seconda categoria rientrano nella famiglia dei cd. "indizi", ossia – come suggerisce l'etimo "*index*" – indici o tracce del fatto da provare[56]. Entrambe risultano tuttavia mosse

---

[51] Cfr. M. Chiavario, *Diritto processuale penale*, Wolters Kluwer, Milano, 2019, pp. 445-446, M. Chiavario, *Considerazioni sul diritto alla prova*, in AA.VV., *Studio sul processo penale in ricordo di Assunta Mazzarra*, (a cura di) A. Gaito, Padova, Cedam, 1996, pp. 27 e ss., F. Cordero, *Procedura penale*, Giuffrè, Milano, 2003, p. 570, F. Cordero, *Tre studi sulle prove penali*, Giuffrè, Milano, 1963, p. 52, ove l'Autore la definisce «ciò che si usa al fine di provare», P. Tonini, *La prova penale*, Cedam, Padova, 2000, G. Ubertis, *La prova penale. Profili giuridici ed epistemologici*, Giappichelli, Torino, 1995, G. Ubertis, *La conoscenza del fatto nel processo penale*, Giuffrè, Milano, 1992, M. Nobili, *Concetto di prova e regime di utilizzazione degli atti nel nuovo codice di procedura penale*, in *Foro it.*, 1989, c. 274 e M. Nobili, *Il nuovo 'diritto delle prove' ed un rinnovato concetto di prova*, in *Leg. pen*., 1989, pp. 395 e ss. Giova, peraltro, distinguere la "fonte di prova", intesa come «le persone o le cose da cui la prova può essere tratta», dal "mezzo di prova", ossia il «cosiddetto "fatto rappresentativo"» di cui ci si serve per ottenere la dimostrazione di un accadimento, dal "risultato di prova", inteso come «cosiddetto "fatto rappresentato"». Cfr. M. Chiavario, *Diritto processuale penale*, 9° ed., cit., pp. 445 e ss.

[52] Cfr. L. Saponaro, *L'impatto processuale delle immagini*, cit., p. 21.

[53] Cfr. P. Tonini, C. Conti, *Il diritto delle prove penali*, cit., p. 45.

[54] Cfr. G. Ubertis, *La prova penale. Profili giuridici ed epistemologici*, Utet, Milano, 1995, p. 42, L. Saponaro, *Dall'indizio alla prova indiziaria: il rapporto tra probabilità e certezza*, Wolters Kluwer, Milano, 2015, F. Cordero, *Tre studi sulle prove penali*, cit., pp. 7 e ss. e P. Ferrua, *La prova nel processo penale. Vol. I. Struttura e procedimento*, Giappichelli, Torino, 2017, pp. 65 e ss.

[55] Cfr. M. Bargis, *Compendio di Procedura penale*, Wolters Kluwer, Milano, 2019, p. 267.

[56] «(…) esistono tre *species* di risultati indiziari: gli "indizi semplici" che rappresentano criteri ermeneutici di ricerca utili, soprattutto, nella fase investigativa; le "prove frammentarie" che sono "principi presuntivi" di prova e costituiscono il presupposto

dalla stessa finalità e tendono verso lo stesso risultato: l'accertamento del fatto storico. La cifra distintiva risulta riferibile, invece, unicamente «all'esplicazione pratica dell'aspetto rappresentativo sul quale si riflette il procedimento gnoseologico giudiziale»[57].

Posta tale distinzione, risulterà naturale chiedersi ove si collochi, nel presente scenario, il risultato di compatibilità espresso in termini probabilistici scaturente da un software automatico e quale possa essere il suo effettivo valore probatorio (cfr. *infra* il § 1.3). Si badi bene, ciò su cui interessa focalizzare la ricerca non è tanto la portata dimostrativa della rappresentazione digitalizzata di un dato biometrico in sé[58], quanto del *match* fra due dati biometrici digitalizzati, ottenuto tramite l'impiego di uno strumento computazionale. In altre parole, prendendo in considerazione il risultato positivo di compatibilità fra una combinazione di rappresentazioni digitali di uno stesso tratto biometrico, si vuole incentrare l'analisi sulla sua capacità dimostrativa nel processo[59]. A tal proposito, quanto incidono il grado di invariabilità o quello di singolarità del campione biometrico grezzo, oggetto di rappresentazione digitale impiegata a fini di comparazione (cfr. il capitolo I, § 1.2)? E ancora, quale grado di inferenza presuppone il risultato scaturente da un sistema automatico di riconoscimento e qual è, rispetto ad esso, la probabilità di derivazione del fatto ignoto nel quale si identifica il tema di prova?[60]

In secondo luogo, un aspetto strettamente connesso a quello presentato concerne la verifica dell'*attendibilità ontologica* di un risultato scaturente da un software automatico di riconoscimento. Ogniqualvolta venga introdotta nel processo una nuova prova scientifica, il problema fondamentale che deve affrontare il giudice – ma, a diverso titolo, anche il pubblico ministero e le parti private – riguarda, come accennato poc'anzi, l'affidabilità della teoria tecnica o metodo scientifico applicati[61]. La problematica interessa cosa può essere definito "scientifico", nel senso che una prova scientifica è veramente tale solo se affidabile[62]. Ebbene, risulta concretamente possibile - ad oggi - contestare l'attendibilità di un *match* automatico? Oppure il risultato di compatibilità espresso in percentuale

---

di provvedimenti che incidono su diritti di libertà del singolo; le "prove indiziarie" che sono le vere e proprie prove critiche». L. Saponaro, *Dall'indizio alla prova indiziaria,* cit., p. 14.

[57] Cfr. L. Saponaro, *L'impatto processuale delle immagini*, cit., p. 26. «In un caso il giudice ricostruisce, in un atteggiamento neutrale, il giudizio storico che l'atto o la cosa sono intesi a comunicare; poi verifica se il messaggio sia veritiero. Nell'altro, non si chiede all'operatore di controllare un giudizio altrui, ma di esprimere il proprio, muovendo a ritroso dalla percezione di un fatto, secondo le leggi dell'esperienza e della logica». F. Cordero, *Tre studi sulle prove penali*, cit., p. 17.

[58] Sul valore probatorio delle immagini in generale cfr. L. Saponaro, *L'impatto processuale delle immagini: fotografie e videoriprese*, Wolters Kluwer, Milano, 2020.

[59] A titolo esemplificativo, qual è il valore probatorio di una corrispondenza (cd. *match*) fra un'immagine digitale ritraente il volto estrapolato da un *frame* di un filmato di videosorveglianza contente la riproduzione oggettiva di un evento e un'altra contenuta in un database?

[60] Su questo punto si tornerà *infra* al § 1.2.1.

[61] Cfr. su questo punto R.V.O. Valli, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, in *Il Penalista*, 16.1.2019.

[62] Cfr. *supra* il § 1.1.

risulta ontologicamente "impermeabile"[63] al confronto dialettico tra le parti? Le questioni che qui si pongono quindi, come oggetto centrale della riflessione e su cui si tornerà meglio *infra*, concernono non solo l'accertamento della sussistenza o meno della capacità semantico-dimostrativa di un *match* rispetto al procedimento[64], ma anche la verifica dell'accuratezza/attendibilità del dato generato e/o processato tramite uno strumento computazionale. In effetti, un altro tema concernente la prova dotata di elevato tasso di scientificità è rappresentato proprio dalla concreta possibilità di dare applicazione al principio del contraddittorio, peraltro consacrato – come si approfondirà meglio *infra* (§ 2.2.) – anche a livello costituzionale[65]. L'art. 111 Cost. ha cristallizzato infatti tale canone sia nel suo aspetto oggettivo, ossia come metodo di accertamento, sia nel suo aspetto soggettivo, che si delinea come garanzia individuale[66]. La valorizzazione del metodo dialettico – che il nostro sistema processuale oggi prevede anche a seguito dell'introduzione a livello costituzionale del principio della formazione della prova nel contradditorio delle parti – obbliga ad un sempre più adeguato controllo critico dei risultati. Tuttavia, di fronte ad un dato generato e/o processato esclusivamente tramite uno strumento computazionale, la realizzazione del contraddittorio tra le parti nel processo, circa il funzionamento esatto del *tool* automatizzato, non risulta sempre possibile, generando certamente una situazione di squilibrio conoscitivo tra le stesse.

In generale, l'ingresso di conoscenze specialistiche nel processo risulta già di per sé poco equilibrato, dal momento che, come è stato rilevato in dottrina, in genere «una delle parti – per lo più quella pubblica – ha accesso alla scienza e alle tecnologie migliori, disponendo di mezzi economici non limitati»[67]. Per vero, «il fenomeno di *knowledge impairment* non è nuovo e ogni stagione del complicato rapporto tra scienza e processo penale ne ha riproposta una versione più o meno intensa (si pensi al debutto della profilazione del DNA nelle aule di giustizia, o al ricorso alla fMRI per l'accertamento di profili legati all'imputabilità)»[68]. Il trattamento automatizzato di alcune tipologie di modello elettronico biometrico e, più in generale, della prova algoritmica *tout court*, tende a estremizzare tale fenomeno, dal momento che l'inaccessibilità di determinate caratteristiche dei

[63] Aggettivo che si ritrova in S. Quattrocolo, *Equo processo e sfide della società algoritmica*, cit., p. 138.

[64] Cfr. *ex multis*, S. Quattrocolo, *Equo processo e sfide della società algoritmica*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2019, p. 138 e AA.VV., *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations*, (a cura di) M. Caianiello, A. Camon, Wolters Kluwer, Milano, 2021, p. 19.

[65] Cfr. L. D'Auria, *Prova penale scientifica e 'giusto processo'*, in *Giust. pen*., 2004, I, 20 e, ampiamente, O Dominioni, *La prova penale scientifica*, cit., pp. 262 ss. sull'esercizio del contradditorio nel giudizio.

[66] «Il comma 4, primo periodo, stabilisce che il processo penale è regolato dal principio del contraddittorio nella formazione della prova; in tal modo, la disposizione dà una prescrizione di natura oggettiva. (…) Al tempo stesso, il comma 3 riconosce all'imputato la facoltà di interrogare davanti al giudice le persone che rendono dichiarazioni a suo carico. La norma chiaramente dà una prescrizione di tipo soggettivo, funzionale alla tutela dell'imputato». P. Tonini, *Progresso tecnologico, prova scientifica e contraddittorio*, in AA.VV., *La prova scientifica nel processo penale*, (a cura di) L. De Cataldo Neuburger, Cedam, Padova, 2007, p. 64.

[67] Cfr. S. Quattrocolo, *Equo processo e sfide della società algoritmica*, cit., pp. 138-139.

[68] Cfr. S. Quattrocolo, *Equo processo e sfide della società algoritmica*, cit., p. 139.

software utilizzati non consente alla parte di falsificarne o quantomeno contestarne l'accuratezza[69]. D'altro canto, la componente tecnico-scientifica della prova non può sottrarre questa al rispetto delle garanzie difensive e alla salvaguardia dei diritti fondamentali delle parti coinvolte. Ciò posto, i problemi scaturenti dal trattamento di dati generati o processati automaticamente per finalità giudiziarie risultano piuttosto evidenti. Il rischio prospettato, tra l'altro, è quello di una lenta e inarrestabile deprivazione dei soggetti del processo del loro ruolo all'interno dell'*iter* procedimentale probatorio, posta ancora più in evidenza dall'assenza di una chiara normativa di riferimento sul tema[70]. Forse, l'approccio di una costante tensione tra scienza e processo penale verso l'elaborazione di regole di cui il secondo dovrebbe dotarsi per dominare in modo corretto la conoscenza scientifica andrebbe invertita. L'approccio suggerito negli ultimi anni da parte della dottrina si interroga su come la scienza – nel momento in cui diviene strumento utile per l'accertamento dei fatti – debba modellarsi tenendo conto delle dinamiche e delle regole del processo e non viceversa[71]. Tuttavia, l'adozione di questo criterio non è sempre possibile e pragmaticamente realizzabile, dal momento che, anche grazie all'introduzione delle tecniche di intelligenza artificiale impiegate a partire dalla prima fase delle indagini preliminari (v. il § successivo), il progresso scientifico risulta continuo e incessante e, per tale ragione, la legge processuale fatica nell'avanzare la pretesa di appropriarsene in un repertorio esaustivo cristallizzato[72]. Come è stato sottolineato, «l'importante è che la prova scientifica, nel momento in cui entra nel processo penale, ne rispetti – e non è sempre agevole – le fondamentali regole rappresentate, per quanto riguarda la formazione della prova, dal contraddittorio e, per quanto riguarda la valutazione, dall'esigenza che il sapere altamente specialistico, veicolato dalla prova scientifica, sia reso pienamente accessibile al giudice, come alle parti, pena il rischio che, altrimenti, la sentenza si riduca alla mera recezione di scelte altrove deliberate» (cfr. *infra* i §§ 1.1.2 e ss.)[73].

[69] Su questo punto si tornerà meglio *infra* al § 2.2.

[70] «Il dato, raccolto o elaborato digitalmente rischia di divenire di per sé attendibile perché la verificazione del processo che lo ha generato è troppo complessa o sfugge, almeno in parte, per via del ricorso a forme più o meno sofisticate di intelligenza artificiale, ad un controllo *ex post*. In tale quadro, l'accusa ha accesso, per evidenti ragioni, alla migliore tecnologia, i cui risultati vengono trasferiti nel processo penale come prove. La difesa, per le ragioni sopra esposte, non ha la possibilità di mettere convincentemente in dubbio l'attendibilità di tale prova, poiché non ha gli elementi necessari alla falsificazione. Il giudice, per parte sua – soprattutto in quegli ordinamenti più nettamente ispirati al principio dispositivo della prova - può non avere motivo di dubitare di tale prova, in assenza di elementi concreti addotti dalla difesa, 'adagiandosi' sul convincimento che il dato digitale sia scevro da rischi di inaccuratezza». S. Quattrocolo, *Equo processo e sfide della società algoritmica*, cit., p. 141.

[71] Cfr. S. Renzetti, *La prova scientifica nel processo penale: problemi e prospettive*, in *Rivista di Diritto Processuale*, 2/2015, p. 399 e G. Ubertis, *Il giudice, la scienza e la prova*, in *Cass. pen.* 2011, p. 4111.

[72] Non è possibile perché la velocità dell'evoluzione tecnologica è superiore rispetto ai tempi di applicazione, monitoraggio e valutazione necessari per una loro concreta verifica. O. Dominioni, *La prova penale scientifica*, cit., p. 26, A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, cit., p. 86 e S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Springer, Cham, 2020, p. 5.

[73] Cfr. P. Ferrua, *La prova nel processo penale.*, cit., p. 302.

1.1.2 Le indagini preliminari come *sedes materiae* degli strumenti tecnico-scientifici

Come noto, il tema del rapporto fra scienza e diritto non si esaurisce nella fase squisitamente processuale[74]. Invero, esso riguarda soprattutto quella parte del procedimento penale in cui la prova scientifica viene a formarsi sempre più di frequente – le indagini preliminari – e quel complesso di problematiche giuridiche legate alla sua introduzione[75]. Il maggiore ricorso a strumenti tecnologici, infatti, si registra nella fase investigativa iniziale, laddove la polizia giudiziaria, il pubblico ministero e i consulenti tecnici adottano strumenti di elevata specializzazione e conoscenze scientifiche di ultima elaborazione[76]. Proprio durante le indagini preliminari viene generata sempre più spesso la vera e propria prova a contenuto scientifico[77]: l'avvento di tecnologie sempre più sofisticate nel procedimento penale sta così determinando una complessa rivoluzione delle tradizionali categorie processuali[78]. Attraverso l'impiego di software, nei quali - come visto - sempre più di frequente sono applicate tecniche di IA, in grado di riconoscere soggetti o captare segretamente flussi di conversazioni, flussi telematici e dati digitali di diversa natura, gli organi inquirenti dispongono di un'amplissima gamma di azioni a tratti estremamente intrusive, sconosciute fino a pochi anni fa. Ma non solo, da tutti i supporti digitali, anche quelli aventi finalità del tutto estranee al procedimento penale, come già accennato *supra*[79], è possibile estrarre molteplici informazioni di rilievo per dirigere le indagini: le potenti memorie dei dispositivi digitali sono archivi di informazioni e, talvolta, anche

[74] Sul punto si veda T. Alesci, *Il corpo umano come fonte di prova*, cit., p. 44. Per un approfondimento sull'ingresso della scienza nelle indagini preliminari si vedano, *ex multis*, D. Curtotti, L. Saravo, *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze, logica*, Torino, Giappicchelli, 2019, p. 13, AA.VV., *Le indagini atipiche*, (a cura di) A. Scalfati, Giappichelli, Torino, 2019, S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, pp. 205 e ss., S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.* 2/2015, pp. 760 e ss., F. Casasole, *Le indagini tecnico-scientifiche: un connubio tra scienza e diritto in perdurante attesa di disciplina*, in *Dir. Pen. e Processo*, 2008, 11, p. 1443, R.V.O. Valli, *Le indagini scientifiche nel procedimento penale*, in AA.VV., *Il processo penale accusatorio*, (a cura di) E. Stefani, Giuffè, Milano, 2013, pp. 756 e ss.

[75] Cfr. T. Alesci, *Corpo dell'imputato (fonte di prova nel processo penale)*, in *Digesto delle Discipline Penalistiche*, Utet, Milano, 2018, p. 80.

[76] F. Casasole, *Le indagini tecnico-scientifiche*, cit., pp. 1443 e ss. e S. Smyth, *Biometrics, surveillance and the law. Societies of restricted access, discipline and control*, Routledge, New York, 2019, p. 65, la quale afferma che «*law enforcement can be seen as the birthplace of biometrics*». Cfr. anche S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Springer, Cham, 2020, p. 5. Giova peraltro specificare che la polizia, procedendo anche ad atti a valenza tecnico-scientifica, può servirsi delle proprie strutture specializzate o di esperti esterni. Come è stato evidenziato, non è del tutto chiaro però se le «persone idonee» menzionate nell'art. 348 c.p.p. debbano intendersi come esperti esterni alle strutture di polizia (per es. un laboratorio pubblico di analisi) ovvero di esperti interni (per es. la divisione di polizia scientifica). Per una lettura critica del punto cfr. B. Lavarini, *Elementi di procedura penale*, cit., pp. 119 e ss.

[77] Cfr. T. Alesci, *Corpo dell'imputato (fonte di prova nel processo penale)*, cit., p. 80 e F. Nicolicchia, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Wolter Kluwer, Milano, 2020, pp. 11 e ss.

[78] Cfr. F. Palmiotto, *Le indagini informatiche e la tutela della riservatezza informatica*, in *www.lalegislazionepenale.it*, 1.7.2019, p. 2.

[79] Cfr. il capitolo II, § 1.

di elementi di prova. Ci si riferisce sia ai dati sia ai cd. metadati, ossia informazioni circa le condizioni oggettive di genesi dei dati stessi[80]. Sempre più spesso le informazioni possono essere generate anche automaticamente senza alcun trattamento o intervento umano, da parte di dispositivi di uso quotidiano (per es. assistenti vocali). I dati, inoltre, possono essere trasposti da strumenti analogici a digitali[81], ovvero possono essere soggetti a particolari trattamenti tecnici[82] al fine di poter compiere delle comparazioni con altri contenuti in ampi archivi di dati o in dispositivi digitali. Invero, l'accesso a determinate informazioni ivi contenute può fornire agli organi inquirenti elementi essenziali per orientare, soprattutto nelle fasi iniziali, la ricerca di elementi di prova. Peraltro, l'estrema rilevanza di tale segmento procedimentale, tenuto conto della sua idoneità a giungere in fase dibattimentale, impone l'adozione di specifici protocolli operativi riguardanti sia le modalità con cui vengono impiegate le tecniche di accertamento, sia la repertazione e la conservazione dei materiali analizzati (cfr. il capitolo II, § 1.2). Questo costituisce in modo ineludibile il basilare e necessario antecedente della fase valutativa, arrivando ad incidere talvolta anche drasticamente sui suoi contenuti e sugli esiti del processo[83]. La rilevanza dell'apporto scientifico, emergendo già in fase investigativa, da un lato costituisce un indiscusso vantaggio per chi se ne serve[84], dall'altro può nascondere alcune insidie e fragilità. Il dibattimento o, ancora prima l'udienza preliminare, rimangono le sedi principali nelle quali viene effettuato il contraddittorio sulla prova e ove viene chiesto ai periti e consulenti un risultato tecnico-scientifico che abbia ad oggetto le attività eseguite nel corso delle investigazioni sia sotto forma di atti irripetibili, sia di rilievi oppure di accertamenti ripetibili. Molti dei problemi giuridici insiti nella prova formata sulla scena del crimine spesso sono poi legati al vuoto normativo all'interno del codice di rito che "aleggia" intorno a certe pratiche investigative, con conseguenti e proporzionali ricadute in sede di formazione del convincimento del giudice. Come già rilevato dalla dottrina[85], la realtà investigativa delle attività tecnico-scientifiche sta assumendo dimensioni sempre più "inedite" che il legislatore del 1988 non era in grado di prevedere. Per vero, che il progresso scientifico abbia fatto prepotente ingresso nella fase delle indagini preliminari è un assunto ormai evidente. Dalle tecniche di reperimento di minime tracce biologiche nella *scena criminis*[86] al metodo della *Bloodstain*

[80] Per una definizione cfr. *ex multis* T. Taulli, *Artificial Intelligence Basics*, Apress, Berkeley, 2019, p. 37.

[81] Per esempio un dato grezzo può subire un procedimento di digitalizzazione da parte degli organi inquirenti a fini di comparazione con altri modelli elettronici della stessa tipologia di dato (cfr. il capitolo I, § 2.2).

[82] Basti pensare al trattamento di un filmato di videosorveglianza dal quale è possibile ritagliare dei *frames* raffiguranti i tratti somatici di un individuo dai quali, a loro volta, ricavare le *features* per la creazione del modello elettronico biometrico o semplicemente per la rappresentazione digitale delle stesse.

[83] D. Curtotti, L. Saravo, *Manuale delle investigazioni sulla scena del crimine.*, cit., p. 13.

[84] R. Lopez, *La rappresentazione facciale tramite software*, in AA.VV., *Le indagini atipiche*, (a cura di) A. Scalfati, Giappichelli, Torino, 2019, pp. 250 e ss.

[85] D. Curtotti, L. Saravo, *Manuale delle investigazioni sulla scena del crimine.*, cit., p. 16.

[86] A tal proposito, si veda A. Fiori, *Mito, realtà e fallacie del Dna (nella pratica) forense*, pp. 1329 ss., L. Pascali, *L'uso del Dna-profiling nel procedimento penale: fatti e misfatti*, pp. 1339 ss., S. Salardi, *Dna ad uso forense: paladino di giustizia o reo di*

Pattern Analysis c.d. BPA (in italiano, analisi delle macchie di sangue), attraverso lo studio della morfologia di schizzi, gocce e macchie presenti sulla scena del crimine[87], dall'uso della disciplina della termografia per consentire di rilevare la temperatura delle singole abitazioni al fine di orientare le attività di perquisizione degli organi di polizia giudiziaria[88], all'utilizzo di software di riconoscimento facciale basati su processi automatizzati per l'identificazione di eventuali sospettati (cfr. *infra* il capitolo IV). Si tratta di un elenco meramente esemplificativo che rispecchia in parte la forte espansione già in atto, sia sotto il profilo quantitativo che qualitativo di tali inedite attività d'indagine[89]. A tal proposito, i fattori da considerare sono essenzialmente tre. Una prima distinzione riguarda gli atti dei quali l'indagato è a conoscenza e quelli svolti a sua insaputa[90]. Il secondo elemento da tenere presente è la ripetibilità o meno dell'attività considerata ovvero, in quest'ultimo caso, l'irripetibilità originaria (art. 431, comma 1 c.p.p.) o quella sopravvenuta (art. 512 c.p.p.)[91]. Infine, l'ultimo snodo fondamentale concerne la regolamentazione o meno delle attività considerate. Rispetto alla prima classificazione, un adeguato bilanciamento fra potenziale idoneità accertativa e rispetto delle garanzie fondamentali è compiuto in prima battuta dal legislatore e filtrato eventualmente nelle condizioni di ammissibilità nonché nelle modalità acquisitive riportate nelle norme[92]. Con riferimento

ingiustizie?, in *Riv. it. Medicina legale*, pp. 1359 ss. Cfr. anche P. Rivello, *Tecniche scientifiche e processo penale*, in *Cass. pen.*, 2013, pp. 1691 ss. (par. 4), nonché P. Tonini, *Informazioni genetiche e processo penale ad un anno dalla legge*, in *Dir. pen. proc*., 2010, pp. 883 ss. e P. Felicioni, *La prova del DNA: profili giuridici*, in *Dir. pen. proc*., 2008, *Dossier: la prova scientifica*, p. 51.

[87] Cfr. Sez. I, 21.5.2008, n. 31456, in *Cass. pen.*, 2009, p. 1840; in dottrina cfr. D. Vicoli, *Riflessioni sulla prova scientifica: regole inferenziali, rapporti con il sapere comune, criteri di affidabilità*, in *Riv. it. med. leg.*, 2013, pp. 1239 e ss. (al richiamo delle note 14 e 15), P. Fratini, *La bloodstain pattern analysis (BPA) come fonte di prova*, in AA.VV., *Scienza e processo penale - Nuove frontiere e vecchi pregiudizi*, (a cura di) C. Conti, Giuffrè, Milano, 2011, pp. 281 e ss., F. Caprioli, *Scientific evidence e logiche del probabile nel processo per il "delitto di Cogne"*, in *Cass. pen*., 2009, pp. 1867 e ss.

[88] È il noto caso *Kyllo*, giudicato dalla Corte suprema americana nel 2001 (*Kyllo v. U.S.*, 533 U.S. 27 (2001). Nella dottrina italiana cfr. M. Miraglia, *Il IV Emendamento alla rincorsa del progresso: perquisizioni e lotta alla droga nel diritto Usa*, in *Dir. pen. proc*., 2002, pp. 105 e ss.

[89] Parte della dottrina mette in guardia gli operatori del diritto dall'utilizzo di tali inedite strumentazioni, *ex multis*, S. Lorusso, *Il contributo degli esperti alla formazione del convincimento giudiziale*, in *Arch. pen*., 2011, pp. 809 e ss. (che segnala il rischio che la prova scientifica divenga il «nuovo totem di un facile efficientismo giudiziario che evoca ambigui scenari inquisitori di sapore tecnocratico»: p. 818).

[90] Un esempio del primo tipo è rappresentato dall'art. 359 *bis* c.p.p. (prelievo coattivo di campioni biologici su persone viventi), del secondo dall'articolo 266 *bis* c.p.p. (intercettazioni di comunicazioni informatiche o telematiche).

[91] Le attività investigative sulla traccia assumono una diversa veste giuridica, a seconda dell'urgenza dell'esecuzione. Per le attività da compiersi con le garanzie di partecipazione della persona sottoposta alle indagini, si può ricorrere agli accertamenti tecnici irripetibili (art. 360 c.p.p.) oppure all'incidente probatorio (392 c.p.p.). Si tratta di attività che devono attendere i tempi di esecuzione delle procedure richieste per l'attivazione della presenza della difesa. Altrimenti, nel caso di attività da eseguirsi "sul campo", nell'immediatezza della scoperta della fonte di prova, quando non è possibile attendere il difensore dell'indagato per un pericolo di contaminazione o deperimento della fonte stessa, si procede nelle forme degli accertamenti urgenti di polizia giudiziaria (art. 354 c.p.p.), dell'ispezione (art. 244 c.p.p.) o dei rilievi tecnici (art. 348 c.p.p.). Si tratta di attività che destano molti problemi, sia di ordine giuridico che di carattere scientifico. Rispetto a quest'ultimo aspetto, la condizione di incertezza che regna sulle attuali operazioni tecniche finisce per incidere sensibilmente sul grado di affidabilità richiesto in sede processuale.

[92] Sulle garanzie processuali fondamentali si dirà meglio *infra*, §§ 2 e ss.

a tutte e tre le distinzioni richiamate, giova ricordare poi che l'atto che s'intende compiere potrebbe non trovare alcuna disciplina legislativa espressa, classificandolo come *atipico*[93].

Provando a riassumere, pertanto, si avranno[94]:

a) attività svolte in dibattimento attraverso mezzi di prova tipici;

b) attività dibattimentali atipiche;

c) attività svolte durante la fase delle indagini sulla base di una disciplina espressa;

d) atti di investigazione atipici.

Tralasciando per il momento le questioni scaturenti dalle attività atipiche dibattimentali[95], si ritiene – concordemente con parte della dottrina – che uno dei principali nodi problematici del procedimento penale, caratterizzato dai maggiori rischi di lesione dei diritti fondamentali, sia costituito, ad oggi, proprio dalle attività di cui alla lettera d)[96]. Queste ultime si caratterizzano soprattutto per il loro contenuto altamente scientifico/tecnologico. Volendo servirsi di una definizione di massima introdotta nell'ordinamento nordamericano, gli atti che qui interessano sono quelli che, attraverso l'uso della tecnologia, non si limitano unicamente a potenziare le ordinarie capacità percettive degli operatori (*sense-enhancing technologies*), ma conferiscono loro facoltà estranee alla dimensione umana (*sense-replacing technologies*)[97]. Alla prima categoria per esempio si potrebbe accostare l'utilizzo di un binocolo durante un pedinamento per il quale non muta la natura tradizionale dell'attività. Per quanto concerne, invece, le *sense-replacing technologies*, esse vanno assimilate a quei processi di raccolta di dati o immagini che funzionano in modo automatizzato, senza che sia previsto nella fase iniziale di funzionamento l'apporto di alcun essere umano. All'interno di quest'ultima categoria rientrano tutti i software connessi a ingenti banche dati.

Il carattere tecnologico, tuttavia, non è tutto. Tali procedure si distinguono anche per la loro potenziale "finalità probatoria": esse devono, infatti, essere utili a fornire informazioni per orientare o far proseguire le indagini. Peraltro, come già accennato poc'anzi, il ricorso frenetico ai summenzionati atti atipici d'indagine ad alto contenuto tecnologico – in assenza di una corrispondente riflessione sulle garanzie – sta comportando un sensibile e preoccupante slittamento del "baricentro" del processo dal

[93] Manca nella fase delle indagini una norma omologa all'art. 189 c.p.p. che permette di demandare al giudice, nel contraddittorio tra le parti, il compito (normalmente spettante al legislatore) di individuare le modalità acquisitive della prova atipica che ne garantiscano l'idoneità accertativa nel rispetto dei diritti della persona. Per un approfondimento sulle attività di indagine atipica si veda AA.VV., *Le indagini atipiche*, (a cura di) A. Scalfati, Giappichelli, Torino, 2019.

[94] La catalogazione è presente in S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen*., 2/2015, p. 766.

[95] Di cui meglio si dirà *infra* al § successivo.

[96] Per un approfondimento cfr. S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, pp. 255 e ss.

[97] Cfr. G. Di Paolo, *"Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione*, Cedam, 2008, p. 18.

dibattimento al segmento precedente delle indagini: il loro impiego influenza in modo deciso e ineludibile le investigazioni, potendo altresì fondare l'applicazione di misure cautelari e, tenuto conto del loro eventuale utilizzo dibattimentale, può spingere l'accusato ad accedere a riti alternativi[98]. Con riferimento alla possibilità di svolgere liberamente attività di investigazione atipica, si deve dar senz'altro conto di una duplice posizione dottrinaria e giurisprudenziale. La risposta più tradizionale parte dall'analisi del Progetto preliminare al codice di rito attualmente vigente, ove si immaginava che, per l'iniziale fase delle indagini preliminari, valessero i principi di "informalità" e "atipicità" che, ad oggi, permetterebbero il ricorso ad atti investigativi innominati[99]. Tale assunto non può reggere rispetto a tutti quegli atti caratterizzati da un elevato contenuto tecnologico, potenzialmente in grado di ledere molteplici diritti fondamentali[100]. Invero, con riferimento a tali attività, si ammetterebbe che il pubblico ministero e la polizia giudiziaria possano precostituire unilateralmente materiale caratterizzato da una spiccata attitudine probatoria con un'incontrollata costrizione del diritto alla difesa.

La seconda risposta che dottrina e giurisprudenza forniscono a tale *quaestio* muove da una lettura più ampia dell'articolo 189 c.p.p. Esso, come si approfondirà meglio *infra*, è tradizionalmente legato all'idea che nel tempo emergano nuove metodologie e cognizioni scientifiche che, se applicate al procedimento penale, possano condurre verso nuove modalità di accertamento del reato. Ebbene, qui la norma non solo può essere applicata per regolare l'ammissione e l'assunzione in dibattimento della prova atipica (cfr. *infra* i §§ che seguono), ma potrebbe essere analogicamente richiamata anche nella fase delle indagini nel caso di atti d'investigazione atipici[101]. Si ritiene tuttavia che, così intesa, la portata garantista attribuita all'articolo 189 c.p.p. applicato all'eterogenea fase delle indagini venga totalmente meno[102]. Infatti, il contraddittorio giudiziale previsto non potrebbe che essere successivo al compimento dell'attività e funzionale a stabilire l'utilizzabilità in giudizio del materiale probatorio

[98] La dottrina tedesca qualifica gli atti di investigazione atipici caratterizzati da una finalità probatoria e dall'incisione di un diritto fondamentale come attività "a duplice funzione".

[99] Cfr. *Progetto preliminare del codice di procedura penale - Relazione*, Istituto Poligrafico e Zecca dello Stato, 1988. In particolare, la Relazione si riferisce sia agli atti di polizia giudiziaria (p. 191) sia a quelli del pubblico ministero (p. 198), facendo leva sulla necessità di venire incontro alle esigenze di fluidità proprie delle indagini preliminari.

[100] Cfr. S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen*. 2/2015, pp. 760 e ss.

[101] La differenza tra applicazione dell'articolo 189 c.p.p. in fase di indagini e in dibattimento, però, risiederebbe nel momento in cui si colloca il contraddittorio giudiziale. Per gli atti di indagine, esso non potrebbe essere preventivo ma solamente successivo al compimento dell'attività e funzionale a stabilire l'utilizzabilità o meno del materiale probatorio. L'interpretazione poggerebbe le sue basi normative nell'art. 61 c.p.p., secondo cui i diritti e le garanzie dell'imputato si estendono alla persona sottoposta alle indagini. M. Nobili, *Il nuovo diritto delle prove e un rinnovato concetto di prova*, in *Leg. pen*., 1989, cit., p. 399, P.P. Rivello, *La prova scientifica*, cit., p. 24 e ss. e P. Ferrua, *Formazione delle prove nel nuovo dibattimento: limiti all'oralità e al contraddittorio*, cit., p. 60

[102] Cfr. F. Nicolicchia, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Wolter Kluwer, Milano, 2020, pp. 11 e ss.

raccolto. Tale "filtro", posto anche a distanza - magari - di molti mesi dal compimento di quelle attività investigative, non sarebbe dunque più efficace[103].

Un'altra tesi su cui occorre riflettere è quella che auspica l'introduzione di una puntuale regolamentazione, seppur dotata di una necessaria flessibilità, dell'impiego di strumenti inediti d'indagine[104]. Tale normativa dovrebbe essere abbastanza elastica da non dover inseguire affannosamente il vorticoso progresso scientifico e da consentire un equilibrato bilanciamento fra la protezione dei diritti fondamentali, il principio di proporzionalità e le esigenze investigative[105]. Concordemente con quanto già rilevato da parte della dottrina, si ritiene che, con i dovuti adattamenti ai diversi caratteri tipici della fase delle indagini preliminari, un primissimo modello di riferimento da cui partire per tale proposito possa essere individuato proprio nell'articolo 189 del codice di rito[106], veicolo talora decisivo - come si approfondirà meglio *infra* (cfr. i §§ che seguono) - per l'introduzione della prova scientifica cd. "nuova o controversa e di elevata specializzazione".

1.2. *Digital evidence* e prova scientifica

1.2.1 Alcune nozioni preliminari…

Prima di approfondire alcune delle interpretazioni di dottrina e giurisprudenza concernenti possibili catalogazioni della *digital evidence* entro le tradizionali categorie processuali probatorie, si ritiene ragionevole dar conto di alcune nozioni preliminari. La trattazione del rapporto fra processo penale e prova scientifica, in particolare quella «nuova o controversa e di elevata specializzazione»[107] non può non portare l'attenzione sul fondamentale rapporto tra tipicità e atipicità probatoria. Come noto, il primo canone normativo implica che la legge preveda e regoli determinati mezzi di prova in tutte o in alcune componenti della loro struttura. Il secondo riguarda invece casi diversi: la prima ipotesi è che

[103] «(…) così intesa, però, la portata garantistica che si vorrebbe attribuire all'applicazione dell'art. 189 c.p.p. in fase di indagini scema del tutto: se anche il prefigurato controllo giudiziale di utilizzabilità *ex post* fosse effettivo – ma la "bulimia conoscitiva" di stampo inquisitorio della giurisprudenza porta legittimamente a dubitarne – si consente comunque che per mesi e mesi gli organi dell'investigazione possano, al di fuori di qualsiasi cornice o limite preventivo, nonché di qualsiasi controllo giudiziale *in itinere*, conculcare un diritto che le fonti costituzionali e internazionali vorrebbero inviolabile». S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, cit., p. 773.

[104] Cfr. S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, cit., p. 789; sul punto è concorde anche A. Scalfati, *Premessa*, in AA.VV., *Le indagini atipiche*, (a cura di) A. Scalfati, Giappichelli, Torino, 2019.

[105] C'è chi sostiene l'idea di un vero e proprio intervento di riforma e modifica del codice di rito, come per esempio S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale*, cit., p. 789 e ss., ma anche chi considera più opportuna la redazione di protocolli, magari contenuti in regolamenti, che, da un lato, indichino i mezzi tecnico-scientifici concretamente utili e fruibili, dall'altro, siano sottoposti a regolari aggiornamenti, in modo da renderli sempre attuali. F. Casasole, *Le indagini tecnico-scientifiche*, cit., pp. 1443 e ss.

[106] Cfr. S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen*., 2/2015, p. 768.

[107] L'espressione è di O. Dominioni, *La prova penale scientifica*, cit., p. 13, già richiamata *supra*, cfr. nota n. 28.

si utilizzi un certo strumento probatorio tecnico-scientifico che non si trova nel catalogo legale (mezzo di prova interamente "innominato"); la seconda situazione che può verificarsi è che una componente tipica di un mezzo di prova sia sostituita con una tipica di un altro mezzo di prova (mezzo di prova "irrituale"); infine, può accadere che un mezzo di prova veda una sua componente tipica sostituita con una innominata (mezzo di prova "anomalo"). Secondo una parte di dottrina, la *ratio* di inserire l'atipicità probatoria nel tessuto codicistico andrebbe individuata nell'esigenza di non precludere irragionevolmente la fruibilità processuale dei risultati più nuovi del progresso scientifico[108]. Questo però non significa che tutti i nuovi strumenti tecnico-scientifici siano da considerare espressione dell'atipicità probatoria riconducibili nel novero dell'art. 189 c.p.p.[109]. La tipicità della perizia e della consulenza tecnica, infatti, ruota intorno alle "specifiche competenze" scientifiche e tecniche (nonché artistiche) senza stabilire nulla circa la novità o meno della tipologia di strumento probatorio impiegato, estraneo o regolato dalle previsioni codicistiche. Risulta, dunque, necessario stabilire se e quali contenuti della prova scientifica potrebbero essere ricondotti all'art. 189 c.p.p e quali alle disposizioni del catalogo legale. A tal proposito, parte della dottrina ha proposto due metodi per giungere ad una risposta. Il primo fa leva sulla clausola d'esordio posta nell'art. 189 c.p.p.: essendo tale disposizione riferita alla "prova non disciplinata dalla legge", l'articolo in esame sarebbe stato introdotto per garantire l'accesso alla nuova prova scientifica assicurando e migliorando così l'accertamento del fatto, al punto da costituire il fondamento stesso della sua *ratio legis*[110]. In questo senso, «sono, dunque, due gli oggetti da ricondurre alle previsioni dell'art. 189 c.p.p.: la prova atipica in senso proprio, tale perché si discosta completamente dai modelli legali, e la prova atipica in senso improprio, cioè la prova scientifica nuova, tale perché sconosciuta o non sufficientemente riconosciuta, quanto ad affidabilità, dall'esperienza giudiziaria»[111]. Quanto al secondo metodo, esso si fonda essenzialmente su un'interpretazione analogica della disposizione normativa e della nozione di prova scientifica nuova ad essa accostabile. La *ratio* dell'art. 189 c.p.p. risulterebbe così enucleabile: a) l'idoneità all'accertamento del fatto e la non lesività della libertà morale della persona risultano, per la prova tipica, oggetto di un giudizio *ex lege* che manca per la prova atipica e per la quale l'art. 189 c.p.p. prescrive che sia formulato dal giudicante durante la fase di ammissione; b) tale giudizio deve essere espresso prima dell'assunzione della prova atipica anche per tutelare ragioni di

[108] O. Dominioni, *La prova penale scientifica*, cit., pp. 30 e ss.

[109] Su questo punto cfr. O. Dominioni, *La prova penale scientifica*, cit., pp. 30 e ss. e E. Zappalà, *Il principio di tassatività dei mezzi di prova nel processo penale*, Giuffrè, Milano, 1982, pp. 96 e ss.

[110] Cfr. O. Dominioni, *La prova penale scientifica*, cit., p. 103.

[111] Cfr. O. Dominioni, *La prova penale scientifica*, cit., pp. 103 e 104. Di diversa opinione sono *ex multis* G. Ubertis, *Il giudice, la scienza e la prova*, in *Cass. pen*., fasc.11, 2011, p. 4111B, F. Caprioli, *La scienza "cattiva maestra": le insidie della prova scientifica nel processso penale*, in *Cass. pen*., fasc.9, 2008, p. 3520B, V. Bozio, *La prova atipica*, in AA.VV., *La prova penale*, (a cura di) P. Ferrua, E. Marzaduri, G. Spangher, Utet, Torino, 2008, pp. 66 e ss.

economia processuale; c) infine, l'ultima parte dell'art. 189 c.p.p. stabilisce espressamente che il provvedimento predisponga le specifiche modalità di assunzione al fine di compensare il *deficit* di legalità probatoria derivante dalla mancanza di specifiche disposizioni normative.

L'idoneità della prova ad accertare il fatto e la sua non lesività della libertà morale della persona richiedono necessariamente un vaglio preventivo in fase di ammissione, garantendo in questo modo l'accesso al processo solo a prove che rispettino tali requisiti; le ragioni di economia processuali ben possono essere richiamate di fronte a operazioni probatorie «incontrollabili nella correttezza del loro uso pratico», ovvero lesive «della libertà morale della persona, o ancora tanto sofisticate al punto da essere imperscrutabili per il giudice e le parti e sfuggire così al loro controllo ovvero tali da esercitare una suggestione impropria sul convincimento giudiziale»[112]; infine, posto che alcuni strumenti tecnico-scientifici nuovi possono dar luogo ad adattamenti anche molto marcati delle modalità di assunzione tipizzate nel catalogo del mezzo di prova in cui s'intende impiegarli, occorre che, in mancanza di un'esperienza giudiziaria matura, il provvedimento di ammissione ne predetermini le modalità assuntive atipiche adeguate al caso di specie. Ne consegue quindi che, pur tenendo conto di opinioni dottrinarie non sempre concordanti[113], l'art. 189 c.p.p. potrebbe trovare applicazione, con le dovute cautele cui si faceva cenno poc'anzi, quando s'intenda introdurre nel processo una certa tipologia di prova scientifica nuova, declinata nelle diverse modalità sopra accennate. A titolo esemplificativo e come si approfondirà meglio *infra* (cfr. il § 1.3), quanto appena affermato potrebbe essere una valida ragione per considerare "atipico" il trattamento di un modello elettronico biometrico automaticamente generato. D'altro canto, l'articolo 189 c.p.p. riferisce l'atipicità non solo all'assenza di una previsione legislativa ma anche alla novità del metodo impiegato, che, per la tipologia di prove che qui interessano, risulta ancora in fase sperimentale[114].

---

[112] Cfr. O. Dominioni, *La prova penale scientifica*, cit., p. 105.

[113] Cfr. F. Focardi, *La consulenza tecnica extraperitale delle parti private*, Cedam, Padova, 2003, pp. 185 e ss. in cui l'Autore evidenzia come la distinzione tra scienza ordinaria e *novel science*, pur certamente chiara in astratto, sia in realtà assai "sfuggente" in concreto, dal momento che non sarebbero stati specificati le concrete modalità e i soggetti che possono avanzare una richiesta di prova qualificata come di "scienza nuova". Cfr. ancora G. Ubertis, *Il giudice, la scienza e la prova*, cit., p. 4111B, F. Caprioli, *La scienza "cattiva maestra": le insidie della prova scientifica nel processso penale*, cit., p. 3520B, V. Bozio, *La prova atipica*, cit., pp. 66 e ss.
Sul fronte giurisprudenziale cfr. Cass. pen., Sez. I, 21.5.2008, n. 31456, in *CEDCass* n. 240764 con il commento di F. Caprioli, *Scientific evidence e logiche del probabile nel processo per il "delitto di Cogne"*, in *Cass. pen*., fasc.5, 2009, p. 1867,

[114] Ci si riferisce all'"evidenza automaticamente generata" per es. da un dispositivo IoT (cfr. la classificazione riportata nel capitolo II, § 1). Rispetto alle altre due tipologie di modello elettronico, come si approfondirà meglio *infra* (cfr. il § 1.3), per il momento esse sono destinate a trovare spazio nel vasto filone di tecniche investigative atipiche utilizzate dalla polizia giudiziaria nella fase iniziale delle indagini preliminari.

1.2.2. La *digital evidence* tra tipicità e atipicità probatoria

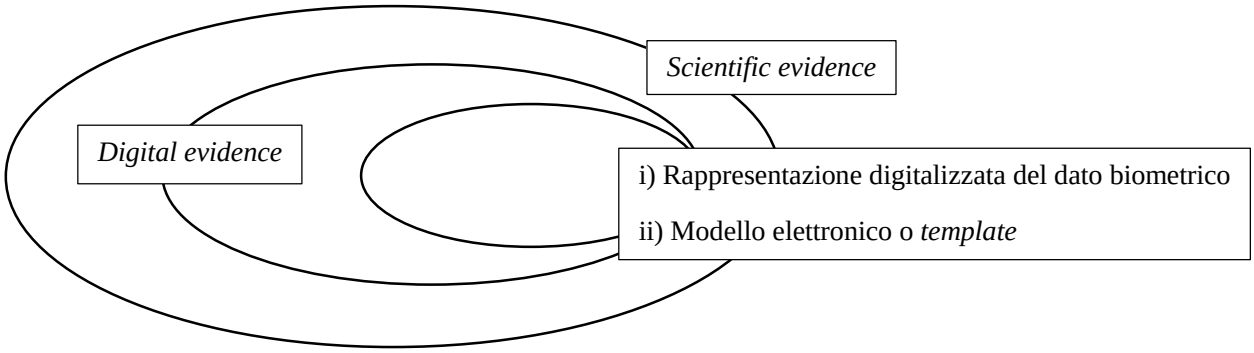
Una volta delineati i tratti tipici della prova tecnico-scientifica con le attenzioni circa le dovute distinzioni fra prova tipica e atipica, è ora possibile approfondire l'inquadramento della *digital evidence*[115] per poi avanzare successivamente, in assenza di interpretazioni giurisprudenziali sul punto, una proposta di categorizzazione del risultato di compatibilità fra le riproduzioni digitalizzate di un dato biometrico (cfr. lo schema n. 2).

Un primo indirizzo dottrinale sostiene che la prova digitale costituirebbe «un sottotipo di recente emersione [della prova scientifica], a causa dell'alto grado di tecnicismo richiesto per trasformare le informazioni - originariamente contenute in macchinari alquanto complessi - in dati intellegibili da un giudice»[116]. Per vero, questa tipologia di evidenza, poiché fondata su tecniche tipicamente riconducibili alla scienza informatica, potrebbe effettivamente essere ricondotta - di primo acchito - nel novero delle prove scientifiche. In effetti, le diverse attività che si svolgono nell'ambito della *digital forensics* esulano dalle competenze dell'uomo medio[117] e coinvolgono necessariamente precise conoscenze tecniche di elevata specializzazione. Tuttavia, come rilevato da altra parte della dottrina, «il tema dell'intreccio tra *scientific evidence* e *digital evidence* è (…) alquanto delicato e merita qualche precisazione in più»[118]. Da una parte, infatti, per il trattamento della *digital evidence*, l'impiego di tecniche scientifiche ad elevata specializzazione risulta essenziale non solo nei momenti di ammissione, assunzione e valutazione della prova, ma anche, in fase investigativa, per l'identificazione stessa del dato conoscitivo e per la sua acquisizione all'interno del procedimento, nonché, in seguito, per l'analisi del dato. Dall'altra, non esiste alcun metodo scientifico che possa portare a risultati certi, potendosi ragionare per lo più in termini di elevata probabilità delle conclusioni. Questo appare ancora più sicuro con riguardo alla rappresentazione di un dato biometrico digitalizzato, a causa dei già accennati particolari tratti che connotano tale tipologia di informazione e che la rendono «quanto mai sfuggente»[119].

Più nel dettaglio, la *digital evidence* pone alcune problematiche rispetto alla sua collocazione nell'ambito del sistema codicistico ovvero, con riguardo alla sua capacità dimostrativa intesa come "prova scientifica", all'attendibilità dei risultati prodotti dall'esperto e al rischio di un'effettiva

[115] Per un approfondimento si fa rinvio integrale alle fonti indicate nel capitolo II, § 1.
[116] Cfr. L. Marafioti, *Digital evidence e processo penale*, cit., p. 4510 e nello stesso senso AA.VV., *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations*, (a cura di) M. Caianiello, A. Camon, Wolters Kluwer, Milano, 2021, p. 15. Di contrario avviso invece F. M. Molinari, *Le attività investigative inerenti la prova digitale*, in *Cass. pen*., 3/2019, p. 1261.
[117] Cfr. P. Perri, *Computer forensics (indagini informatiche)*, in AA.VV., *Dig. pen.*, IV ed., Utet, Torino, 2011, p. 98.
[118] Cfr. M. Pittiruti, *Digital evidence,* cit., p. 15.
[119] Cfr. il capitolo I, § 2.5. L'espressione è di M. Pittiruti, *Digital evidence*, cit., p. 16.

sopravvalutazione del contributo cognitivo di quest'ultimo. Va poi tenuto in considerazione l'ulteriore livello di complessità, nell'inquadramento codicistico, dell'applicazione di tecniche di intelligenza artificiale ai sistemi di riconoscimento biometrico che rendono lo scenario ancora più composito. Per tale ragione, s'intende qui dar conto *in primis* dei diversi indirizzi dottrinali e giurisprudenziali sull'inquadramento normativo della prova digitale e, successivamente, presentare alcuni spunti di riflessione su una proposta di classificazione probatoria, qualora al dato biometrico, inteso in tutte le sue possibili estrinsecazioni poc'anzi accennate (cfr. *supra* il § 1), fossero applicate - a fini di comparazione - tecniche di intelligenza artificiale, posto che, ad oggi, la *sedes materiae* dell'impiego della maggioranza dei sistemi automatizzati di riconoscimento biometrico attualmente in uso sono le indagini preliminari (cfr. il § 1.3.1)[120].



Schema n. 3

In un primo momento, agli albori dell'impiego della *digital evidence* nel processo penale, si era sostenuta la sua riconducibilità, pressoché automatica, alla disciplina contenuta nell'art. 189 c.p.p.[121]. D'altronde, come già fatto cenno, la norma sarebbe stata introdotta con la *ratio* di rispondere alle sfide imposte dal «continuo sviluppo tecnologico che estende le frontiere dell'investigazione»[122].

Tuttavia, ritenere la prova digitale *tout court* annoverabile nel calderone della prova atipica, soprattutto in seguito alle modifiche introdotte dalla l. n. 48/2008, potrebbe sembrare completamente anacronistico, dal momento che diverse norme del codice di procedura penale sono state modificate proprio al fine di superare alcune questioni scaturenti dal trattamento di una prova avente natura

[120] Più nel dettaglio, come si approfondirà meglio *infra*, si ricorre ai sistemi di riconoscimento biometrico 1:N, 1:N+1 come strumento atipico di investigazione al fine di orientare le indagini preliminari. Lo *score* del software viene introdotto nell'*iter* del procedimento probatorio tipico in seguito all'intervento di un operatore esperto che verifichi l'effettivo *match* e compia le dovute misurazioni (1:1) per poter convalidare il risultato del sistema automatico. Cfr. *infra*, il § 1.4.

[121] Cfr. P. Gualtieri, *Prova informatica e diritto di difesa*, cit., p. 70.

[122] Cfr. *Relazione al progetto preliminare del codice di procedura penale*, in G. Conso, V. Grevi, G. Neppi, *Il nuovo codice di procedura penale. Dalla legge delega ai decreti delegati*. Vol. IV, *Il progetto preliminare del 1988*, Cedam, Padova, 1990, pp. 553 e ss.

digitale. Peraltro, già precedentemente all'emanazione della suddetta legge, ci si era posti il dubbio circa la ragionevolezza di ricondurre tutte le ipotesi di prova digitale e, più in generale, di *scientific evidence* nel novero delle prove atipiche[123]. Il che troverebbe conferma proprio con riferimento alla *digital evidence*, rispetto alla quale, anche prima della riforma del 2008, non si era in presenza di un'atipicità probatoria pura, nelle sue consuete accezioni di prova "innominata"[124], prova "irrituale"[125], ovvero prova "anomala"[126]. Infatti, l'aspetto inedito dell'acquisizione della prova digitale è rappresentato dall'oggetto materiale dell'attività probatoria, ossia i dati digitali. Per vero, la *quaestio* riguarda allora «la capacità espansiva degli istituti» - già previsti dal codice - con riferimento ai tratti tipici della *digital evidence* (cfr. il capitolo II, § 1.1). A tal proposito, è stato osservato che, per garantire l'ingresso di strumenti tecnico-scientifici in dibattimento, sarebbe già sufficiente il ricorso a istituti tipici come la perizia, la consulenza tecnica o la prova documentale[127]. Con riferimento a quest'ultima, giova soffermarsi brevemente, ricordando che l'articolo 234 c.p.p. può essere applicato a «strumenti analogici, la cui peculiarità è data da grandezze fisiche che assumono valori continui»[128]. Questo, tuttavia, non ha impedito alla giurisprudenza di legittimità di ricondurre in tale categoria diverse tipologie di dato digitale[129]. Peraltro, l'interpretazione letterale dell'art. 234 c.p.p. sembra compatibile con qualsiasi rappresentazione di fatti, persone, o cose a prescindere dal mezzo utilizzato[130].

In ogni caso, la distinzione tra prova atipica, per cui è richiesto alle parti uno specifico vaglio preventivo, e gli istituti tipici deputati a garantire l'ingresso di conoscenze tecnico-scientifiche, è stata individuata dalla giurisprudenza di legittimità[131], nel peculiare carattere di novità e autonomia del metodo scientifico applicato. Infatti, qualora questo sia oggetto di molteplici esperienze collaudate, non sarebbe necessario un previo contraddittorio fra le parti per l'ammissione della prova, secondo quanto stabilito dall'art. 189 c.p.p. Allora, ne consegue che, dal momento che il trattamento della *digital evidence* fa parte del più ampio ambito scientifico della *computer forensics*, basato su regole informatiche e matematiche intese come discipline universalmente riconosciute, si potrebbe ritenere

[123] Cfr. F. Caprioli, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen*., 2008, pp. 3520 e ss.
[124] Ossia un mezzo di prova del tutto nuovo o non disciplinato dalla legge.
[125] Ossia un mezzo di prova utilizzato diversamente rispetto alle consuete modalità previste dalla legge.
[126] L'espressione indica l'utilizzo di un mezzo di prova per ottenere il risultato di un altro tipico mezzo di prova.
[127] Rispettivamente artt. 233, 220 e 234 c.p.p. Cfr. M. Pittiruti, *Digital evidence*, cit., pp. 20 e 23 e ss.
[128] Cfr. F. Zacchè, *La prova documentale*, Giuffrè, Milano, 2012, p. 26.
[129] Cfr. Cass. pen., Sez. III, 5.7.2012, n. 374119 in *CED Cass* n. 253573, Cass. pen. Sez. VI, 20.12.2018, n. 15838 in *CED Cass* n. 275541 e Cass. pen., Sez. VI, 6.2.2020, n. 12975 in *CED Cass* n. 278808.
[130] Cfr. L. Kalb, *Il documento nel sistema probatorio*, Giappichelli, Torino, 2000, p. 72.
[131] Cfr. *ex multis*, Cass. pen., Sez. I, 21.5.2018, n. 31456, in *Cass. pen*., 2009, pp. 1840 e ss. con nota di F. Caprioli inerente la *Blood Pattern Analysis* (B.P.A.).

che qualsivoglia risultato digitale possa essere introdotto attraverso gli istituti tipici di perizia, consulenza tecnica o documento.

Resta ferma la peculiare natura della *digital evidence* già accennata *supra* (cfr. il capitolo II, § 1.1) che porta con sé un'inconfutabile complessità di tipizzazione da cui deriva una scarsa adattabilità con uno schema probatorio rigido. Questo è stato tenuto in considerazione dalla giurisprudenza di legittimità che ha ritenuto più volte compreso nell'alveo dell'art. 189 c.p.p. qualsiasi strumento di indagine che si discosti dal rigoroso paradigma legale, a prescindere dalla natura del dato da acquisire e, dunque, anche quello digitale[132]. La φύσις del dato non appare dunque di per sé in grado di consentire una collocazione preventiva all'interno delle categorie probatorie tradizionali del codice di rito. Ciò significa che risulta necessaria una verifica caso per caso del dato digitale trattato nella fattispecie concreta: fonte di convincimento inedita o meno rispetto al catalogo legale. Le diverse interpretazioni dottrinarie e giurisprudenziali, nonostante le modifiche legislative, sembrano essere lo specchio allora dell'esistenza di problematiche ancora presenti insite nell'intersezione tra processo e dato digitale[133].

Un aspetto connesso da tenere in considerazione è rappresentato poi dalla collocazione normativa dell'impiego di strumenti utilizzati per il reperimento del dato digitale. In altre parole, è necessario soffermarsi sulla dicotomia fra diritti fondamentali coinvolti e accertamento investigativo e, più generalmente, fra tutela dell'individuo e ricerca della verità. Per vero, proprio il riferimento alla libertà morale contenuto nell'articolo 189 c.p.p. deve orientare il giudice nella rigorosa verifica circa la conformità dello strumento investigativo utilizzato con i diritti fondamentali della persona (cfr. *infra* i §§ 2 e ss.). Inoltre, la potenziale lesione di questi richiama le dovute esigenze di legalità, comprimibili solo nei casi e nelle modalità previste dalla legge, il che risulta in antitesi con i tradizionali tratti della prova atipica, ove la struttura acquisitiva risulta per definizione slegata da determinate disposizioni normative e rimessa al contraddittorio fra le parti (cfr. *infra* il § 2.4). Invero, la giurisprudenza di legittimità non ha sempre mostrato un atteggiamento garantista riguardo all'impiego di nuovi strumenti di indagine[134], preferendo valorizzare piuttosto il principio di non dispersione della prova, con il necessario coinvolgimento di diritti inviolabili quali la libertà personale o il diritto di difesa[135].

[132] Cfr. *ex multis*, Cass. pen., Sez. V, 27.2.2002, n. 16130 in *CED Cass* n. 221918.
[133] Cfr. M. Pittiruti, *Digital evidence*, cit, p. 31.
[134] Cfr. M. Pittiruti, *Digital evidence*, cit., p. 22.
[135] Con riferimento alla rappresentazione digitale del dato biometrico e al suo modello elettronico, si tornerà meglio *infra* ai §§ 2.1 e 2.2.

1.3 Il *match* fra due dati biometrici digitalizzati come oggetto di prova

In assenza di pronunce giurisprudenziali sul punto, occorre domandarsi quale potrebbe essere il possibile formale accesso di un *match* scaturente da un sistema biometrico di riconoscimento automatizzato, inteso *lato sensu*, sul quale siano applicate tecniche di intelligenza artificiale, entro il contesto del procedimento penale. Di più. Occorre chiedersi come assicurare che il risultato di compatibilità fra due dati biometrici digitalizzati - peculiare sottoinsieme di *digital evidence* (cfr. il capitolo II, § 1) - sia effettivamente in grado di implementare la qualità delle performance cognitive e decisionali dell'organo giudicante in conformità al principio del contraddittorio sulla prova e in funzione della sua doverosa validazione scientifica. In tal senso, prima di porre l'attenzione sulle tradizionali categorie del procedimento probatorio, occorre domandarsi cosa rappresenti tale *match* fra diversi modelli elettronici o rappresentazioni digitalizzate del dato rispetto all'oggetto di prova e quale possa essere la sua effettiva capacità dimostrativa in relazione all'accertamento del fatto di reato. Questo costituisce il punto di partenza fondamentale per la proposizione di qualsivoglia futura distinzione normativa. Proprio sulla base di alcune preliminari riflessioni di natura processuale, infatti, sarà possibile analizzare sistematicamente il corretto accesso di tali tipologie di dati all'interno del processo.

Per giungere ad una proposta di classificazione, si ritiene ragionevole muovere dalla definizione, richiamata poc'anzi, del concetto di "prova" e alcune connesse distinzioni. Come già visto *supra* (cfr. il § 1.1), quest'ultima può definirsi tale qualora «si assuma come dimostrazione di un accadimento e/o di sue determinate modalità» - qui intesa come "fatto rappresentato", ovvero, se costituisce «il mezzo di cui ci si serve per ottenere quella dimostrazione»[136]. Oltre a ciò, come visto, il codice di procedura penale evoca diverse volte la categoria concettuale dell'" indizio", quasi a suggerire una sottile diversificazione di quest'ultimo dalla prova in senso stretto, senza tuttavia fornire un univoco criterio di discernimento. A tal proposito, si suole distinguere fra prova rappresentativa (o diretta) e prova critica (o indiretta o logica)[137]: mentre con la prima s'intende la rappresentazione diretta del fatto o dei fatti da provare, la seconda riguarda una circostanza secondaria, dalla quale inferire l'esistenza di un fatto principale tramite una massima di esperienza o una regola probabilistica[138]. Dunque, la prova

[136] Cfr. M. Chiavario, *Diritto processuale penale*, 8° ed., Wolters Kluwer, Milano, 2019, p. 427.

[137] Cfr. *ex multis* G. Lozzi, *Lezioni di procedura penale*, 7° ed., Giappichelli, Torino, 2010, pp. 120 e ss., A. Nappi, *Guida al codice di procedura penale*, 9° ed., Giuffrè, Milano, 2004, pp. 210 e ss. e P. Tonini, C. Conti, *Il diritto delle prove penali*, Giuffrè, Milano, 2014, p. 46.

[138] Le prime si otterrebbero utilizzando esclusivamente leggi logiche o scientifiche non probabilistiche, il che costituisce un altro elemento di differenziazione con gli indizi. Cfr. P. Ferrua, *La prova nel processo penale*, vol. I, Struttura e procedimento, Giappichelli, Torino, 2017, p. 77. Cfr. anche P. Tonini, C. Conti, *Il diritto delle prove penali*, Giuffrè, Milano, 2014, p. 47, J.S. Mill, *Sistema della logica deduttiva e induttiva* (1843), trad. it., Giappichelli, Torino, 1988, II, p. 1143 e F. Cordero, *Tre studi sulle prove penali*, cit., p. 17.

critico-indiziaria risulta dotata di una diversa "immediatezza logica" attraverso la quale il giudice accede alla conoscenza del *probandum*. L'inferenza tramite cui dal fatto secondario si ricava l'esistenza di un fatto principale non ha, però, la funzione di verificare l'attendibilità o la genuinità della fonte, ma quella di formulare un'ipotesi esplicativa che connetta la circostanza indiziante con il risultato probatorio, sulla base di una regola di esperienza in grado di giustificare il passaggio logico. Peraltro, il controllo sull'attendibilità della fonte deve essere comunque compiuto anche nell'ipotesi di prova indiziaria, ma solo rispetto al fatto secondario sul quale s'innesta l'inferenza.

Sulla base di queste prime riflessioni emerge già come la differenza fondamentale fra prove dirette e prove indiziarie pertiene essenzialmente all'oggetto: i mezzi di prova che conducono ordinariamente all'accertamento di un fatto principale (per es. una videoregistrazione o una testimonianza) possono, talvolta, limitarsi ad acclarare l'esistenza di un fatto secondario dal quale è possibile per via inferenziale ricavare il primo. A titolo esemplificativo, s'immagini la circostanza indiziante del rinvenimento di un'impronta digitale nel *locus commissi delicti* in un reato di omicidio, ovvero il suo ruolo come prova diretta qualora il reato per cui si proceda sia quello della violazione di domicilio[139].

Orbene, giova concentrare a questo punto l'attenzione sul *match* fra due dati biometrici digitalizzati scaturente dall'impiego di un software automatizzato. Cosa dimostra di rilevante per l'oggetto di prova un risultato di compatibilità espresso in termini probabilistici fra le *features* di due dati biometrici? Lo *score* restituito da un sistema di riconoscimento è in grado di instaurare un legame diretto con il *thema probandum* ai fini dell'accertamento del fatto di reato nel contesto processuale? Qual è il suo specifico valore semantico rispetto all'oggetto di prova?

È bene partire da un esempio. Supponiamo che:

- Caio è stato vittima di omicidio al parco (fatto principale);
- Ignoto è stato l'unico soggetto ripreso dalle telecamere di videosorveglianza all'uscita del parco (fatto secondario 1);
- per la comparazione dei volti di Ignoto (unico soggetto ripreso dalle telecamere) e Tizio (sospettato) è utilizzato un software di riconoscimento facciale che calcola il grado di similarità restituendo una lista di possibili candidati compatibili con differenti percentuali. Tizio e Ignoto sono compatibili all'80% (fatto secondario 2).

La sola circostanza che Tizio e Ignoto siano somiglianti all'80% presenta qualche attinenza rispetto al fatto principale? Invero, si ritiene che un risultato di tal genere costituisca solamente il frutto di un'ulteriore inferenza, peraltro non avente un contenuto semantico così significativo rispetto allo specifico fatto da dimostrare (cfr. il capitolo I, § 1). A tal proposito, si parla di indizi "di secondo

[139] Cfr. P. Tonini, C. Conti, *Il diritto delle prove penali*, Giuffrè, Milano, 2014, pp. 44 e ss.

grado", con riferimento ai quali, posta una prima conclusione abduttiva a partire da un certo fatto secondario (Ignoto è entrato in contatto con il *locus commissi delicti* o con la vittima), si trae da esso un'ulteriore conclusione (ossia che Tizio sia il responsabile dell'omicidio di Caio) più distante dal fatto principale da dimostrare. Peraltro, la dottrina si è sempre mostrata piuttosto scettica nell'impiego *ad probandum* di questa tipologia di indizi[140], in quanto la probabilità associata all'ipotesi esplicativa decrescerebbe all'aumentare dei diversi passaggi inferenziali attraverso i quali la stessa risulta ottenuta[141]. Il ragionamento di secondo grado avrebbe una base inferenziale talmente incerta che non potrebbe che condurre ad una conclusione ancor meno probabile della prima. Per vero, vi sono dati valutabili dal giudice che, «a causa della loro irrilevanza o intrinseca debolezza, risultano influenti sulla proposizione da provare»[142]. Ne consegue che, come nell'esempio poc'anzi proposto, un risultato scaturente da un software automatico espresso in termini probabilistici non possa in certi casi ritenersi elemento di per sé significativo per la ricostruzione di un fatto di reato, né tantomeno un indice così rilevante ai fini dell'accertamento del fatto. Certamente, esso può assumere però un iniziale valore orientativo per la fase preliminare delle indagini (v. *infra*).

È bene tenere conto di una ulteriore fondamentale prospettiva. Come visto nel capitolo I, i tratti biometrici presentano diverse qualità che variano da dato a dato considerato. Per esempio, il Dna, le impronte digitali e l'iride, avendo ad oggetto un'informazione biologica o biochimica strutturale, permanente e ipervariabile (quindi molto distintiva e tipica) presentano un altissimo grado di "riferibilità individualizzante" (cfr. il § 1.2). Tutte le altre caratteristiche biometriche sono basate su informazioni non permanenti e meno variabili, registrate in un suono o in un'immagine digitalizzata e modellate statisticamente. Queste misurazioni e modelli sono più sensibili ai fattori ambientali (rumore, luce, angolo di cattura, etc.)[143] e quindi meno distintive. Il valore medio-alto della variabilità e, talora, della scarsa qualità di acquisizione del dato pertanto influenzano inevitabilmente anche l'indice di capacità dimostrativa accordata al *match* scaturente dal software automatizzato. Oltre a questo, è bene tenere in considerazione il fatto che, qualora la traccia sia costituita da un profilo completo appartenente ad un unico individuo e per il quale non sussiste la necessità di un'approfondita interpretazione, l'operatore potrà effettuare una mera verifica "formale" sulla compatibilità. Questa però è un'ipotesi eccezionale. Più di frequente, invece, le tracce corrispondono a profili parziali e

[140] Cfr. M. Taruffo, *Certezza e probabilità nelle presunzioni*, in *Il Foro it.*, 1974, p. 83 e L. Montesano, *Le "prove atipiche" nelle presunzioni e negli "argomenti" del giudizio civile*, in *Riv. dir. proc.*, 1980, p. 246.

[141] Cfr. S. D. Poisson, *Recherches sur la probabilitè des jugements en matière criminelle et en matière civile*, Imprimeur – libraire, Parigi, 1837, G. Lozzi, *Lineamenti di procedura penale*, Giappichelli, Torino, 2020, p. 110 e B. Lavarini, *Elementi di procedura penale*, cit., p. 39.

[142] Cfr. P. Ferrua, *La prova nel processo penale*, Giappichelli, Torino, 2017, p. 61.

[143] Cfr. *ex multis* D. Seckinera, X. Malletta, C. Rouxa, D. Meuwly , P. Maynarda, *Forensic image analysis – CCTV distortion and artefacts*, in *Forensic Science International*, 285, 2018, pp. 77–85.

misti[144] per i quali è necessaria una valutazione molto più complessa, che richiede un controllo più approfondito da parte dell'esaminatore forense.

Dal punto di vista, invece, dell'attendibilità di corrispondenza fra i modelli biometrici considerati, diversi software di riconoscimento oggi in uso si esprimono in termini di similarità tra due dati dello stesso tratto biometrico, senza calcolare il risultato in termini di rapporto fra il grado di similarità e di tipicità rispetto ad una "popolazione di riferimento" (cfr. *supra* il capitolo I, § 3.5.1). Senza quest'ultimo valore non è possibile calcolare quanto il campione all'esame sia comune in una data popolazione di riferimento, a discapito del *match* che costituirà sempre - o almeno per il momento, se tali sistemi automatici di riconoscimento rimarranno operativi con queste modalità - un risultato parziale, valutabile al più insieme ad altri elementi di prova[145].

A questo punto della trattazione, occorre stabilire alcune distinzioni di massima. Se si tratta di *match* scaturenti dall'impiego di sistemi di riconoscimento automatizzati fra riproduzioni digitali di dati biometrici ovvero di modelli elettronici delle *features* ricavate da un'immagine digitale, attraverso procedimenti di digitalizzazione, il loro impiego potrebbe rientrare ragionevolmente entro le attività tipiche[146] o atipiche di indagine[147], inquadrabili entro i compiti istituzionali necessari della polizia giudiziaria ai sensi degli artt. 55 e 348 c.p.p., al fine di assicurare le fonti di prova e quant'altro possa servire per l'applicazione della legge penale attraverso la ricerca di ogni elemento utile alla ricostruzione del fatto e alla individuazione del colpevole. In questi casi, infatti, i sistemi automatici di riconoscimento costituiscono uno strumento per lo più d'ausilio per l'esecuzione di una prima "scrematura" tra diversi dati compatibili con quelli appartenenti al soggetto sospettato[148]. Questo si spiega con il fatto che il *match* fra due o più modelli elettronici biometrici non risulta sempre dotato di capacità dimostrativa espressa in termini di forza dell'evidenza rispetto all'oggetto di prova[149]. Per

[144] Appartenenti a individui diversi.

[145] Cfr. per esempio, con riferimento al riconoscimento facciale, *Best Practice Manual for Facial Image Comparison*, pubblicate dall'ENFSI-BPM-DI-01 Version, 01 - January 2018, reperibili all'indirizzo https://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf (visualizzato in data 28.7.2021). In generale, sul tema v. D. Meuwly, D. Ramos, R. Haraksim, *A guideline for the validation of likelihood ratio methods used for forensic evidence evaluation*, in *Forensic Science International*, 276 (2017), pp. 142–153.

[146] Le comparazioni automatiche di impronte digitali nel sistema A.F.I.S.- S.S.A (cfr. il capitolo I, § 3.3.1) o del Dna con l'ausilio della relativa banca dati istituita con l. 85/2009 (cfr. il capitolo I, § 3.6.3) costituiscono ormai un'attività abituale di indagine.

[147] È stata così definita in dottrina l'attività di estrazione e comparazione automatica delle *features* dei volti tramite il software S.A.R.I., inquadrabile come «una sorta di filiazione spuria del riconoscimento fotografico autonomamente curato dalla polizia giudiziaria, a sua volta derivato atipico dell'"atto omologo" del mezzo di prova della ricognizione, disciplinato dall'art. 361 c.p.p.». Cfr. R. Lopez, *Riconoscimento facciale tramite software e individuazione del sospettato*, in AA.VV., *Pre-investigazioni*. (*Espedienti e mezzi*), (a cura di) A. Scalfati, Giappichelli, Torino, 2020, pp. 311 e ss.

[148] Come visto *supra* al capitolo I § 3.5.1, questo non vale per il riconoscimento automatico o semi-automatico del parlatore o per i software di comparazione del Dna che possono essere oggetto di libera valutazione da parte del giudice dibattimentale senza previa verifica di un operatore esperto poiché la tecnologia attualmente in uso è in grado di calcolare il cd. "rapporto di verosimiglianza" rispetto ad una popolazione di riferimento.

[149] Cfr. sul punto V. Guarriello, *L'intelligenza artificiale tra profili giuridici ed alcune delle più attuali applicazioni al servizio della società*, reperibile all'indirizzo https://arsg.it/?p=1781 (visualizzato in data 27.7.2021).

acquisire un legame, seppur di "secondo grado", con il *thema probandum* è necessario un confronto manuale da parte di un operatore esperto[150], il quale applica una metodologia di comparazione/misurazione manuale, conforme agli standard e procedure elaborati dalla comunità scientifica di riferimento, atta a stabilire se due modelli elettronici o rappresentazioni digitali del medesimo tratto biometrico appartengano effettivamente o meno alla stessa persona. Su questo aspetto, tuttavia, sorgono ulteriori dubbi circa l'effettiva capacità del giudice nel valutare comunque il giudizio formulato dall'esperto e l'attendibilità sulla specifica metodologia impiegata (cfr. *infra* il § successivo)[151]. Oltre a ciò, i software automatizzati attualmente in uso non sembrano ancora offrire garanzie efficaci sul piano della conformità a significative precauzioni metodologiche per assicurare la validità scientifica e l'attendibilità delle procedure utilizzate[152].

Sulla base di quanto finora esposto, siamo in grado di tracciare una fondamentale distinzione rispetto al trattamento del dato biometrico digitalizzato. Da una parte, vi sono tecniche investigative in grado di produrre elementi di prova suscettibili di utilizzo processuale, o, in altri termini, informazioni dotate di una capacità dimostrativa tale da essere portatrici di un valore semantico significativo rispetto al *thema probandum*.

Principali dati biometrici impiegati a fini di repressione dei reati (cfr. il capitolo I, § 3)	**Possibilità di implementare tecniche di IA ai sistemi di riconoscimento attualmente in uso dalle forze di polizia in Italia**	**Metodo di comparazione utilizzabile durante le indagini preliminari**	**Metodo di comparazione in dibattimento Schema n.**
Impronte digitali	✓	1:N, 1:N+1	1:1 (almeno 16 *minutiae*)
Volto	✓	1:N, 1:N+1	1:1 (confronto fisionomico)
Geometria della mano	✗	-	-

[150] Ai sensi degli artt. 220 e 233 c.p.p. (cfr. *infra* il § 1.3.1).

[151] Cfr. P. De Hert, *Biometrics: legal issues and implications*, in *Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla*, European Commission, January 2005, p. 39.

[152] Cfr. E. Currao, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Diritto Penale Uomo*, 19.5.2021, p. 21, R.V.O. Valli, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, in *Il Penalista*, 16.1.2019 e E. Mordini, *Ethics and Policy of Forensic Biometrics*, in AA.VV., *Handbook of Biometrics for Forensic*, (a cura di) M. Tistarelli, C. Champod, Springer, Cham, 2017, pp. 360 e ss.

Impronta palmare	✓	1:N, 1:N+1	1:1
Iride / Retina	✗	-	-
Voce	✓	1:N, 1:N+1 (attualmente in fase di progettazione e implementazione)	1:1 o 1:N+1
Firma	✗	-	-
Andatura	✗	1:1	1:1 (misurazione antropometrica)
Dna	✓	1:N, 1:N+1	1:1 (art. 23, d.P.R. 7 aprile 2016, n. 87) ma, 1:N+1, in grado di eseguire il calcolo *LR*

Schema n.4

Dall'altra, sussistono tecniche di indagine che, impiegando i modelli elettronici o rappresentazioni digitalizzate di dati biometrici in software automatizzati di riconoscimento, possono offrire unicamente alcuni spunti investigativi utili per gli organi inquirenti, al fine di indirizzare correttamente le indagini e agevolarne così il loro svolgimento facilitando per esempio l'individuazione di un possibile autore di reato[153].

Rispetto al *match* generato automaticamente, per esempio, da un dispositivo IoT, si è già evidenziato come esso possa costituire un'informazione di grande rilievo per il procedimento penale (cfr. il capitolo II, § 1). Tale tipologia di dato si forma al di fuori del procedimento come "*computer derived evidence*", senza alcun intervento umano nella sua rilevazione poiché scaturente da oggetti di uso quotidiano collegati alla rete internet (cfr. il capitolo II, § 1). A differenza delle prime due tipologie, dunque, il sistema tramite il quale viene originato il modello biometrico di riferimento ha finalità completamente estranee al procedimento. Cionondimeno esso può rappresentare un patrimonio conoscitivo fondamentale per la direzione delle indagini e per il procedimento penale: si pensi, ad esempio, all'impronta digitale o al volto registrati all'interno di uno *smartphone* impiegati per sbloccare il dispositivo. Il software installato è in grado di fornire determinate informazioni agli

[153] Tale distinzione è già presente in R.V.O. Valli, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, cit.

investigatori che indagano su una fattispecie di reato commessa nel luogo in cui il dispositivo è stato ritrovato[154]. Il software presente nella maggior parte dei dispositivi di uso commerciale si limita ad autenticare l'individuo precedentemente registrato, in modalità 1:1[155]. Generalmente, questi dispositivi, sfruttando tecniche di apprendimento automatico, sono in grado di eseguire le comparazioni fra i dati biometrici forniti a partire dalla registrazione della semplice immagine digitalizzata, senza dover ricorrere all'ulteriore trasformazione della stessa in un modello elettronico o *template*.

Come visto *supra* al capitolo II § 1, questa tipologia di dato generato automaticamente può ragionevolmente annoverarsi entro la più ampia categoria di *digital evidence*, per l'analisi del quale valgono i principi fondamentali della *computer forensics* e, tra questi, quelli posti a presidio del recupero della prova digitale per estrapolare informazioni utili dalla sua analisi, preservandone l'integrità[156]. Proprio con riferimento alla cd. *chain of custody* prevista per le indagini informatiche e telematiche, s'intende qui fare completo rinvio al capitolo II, ove la riforma della l. 48/2008 è già stata oggetto di approfondimento.

Come la *digital evidence*, questa tipologia di dato biometrico digitalizzato costituirebbe un "sottotipo" di recente emersione della prova tecnico-scientifica «a causa dell'alto grado di tecnicismo richiesto per trasformare le informazioni – originariamente contenute in macchinari alquanto complessi – in dati intellegibili da un giudice»[157]. A differenza però della prima, il modello elettronico automaticamente generato non è stato ancora oggetto di un vaglio da parte della giurisprudenza rispetto né alla sua corretta collocazione codicistica né alla sua affidabilità intrinseca. La *quaestio* deve allora essere ancora una volta analizzata attraverso i due angoli visuali tramite i quali si sono approfondite le prime due tipologie di dato. Da una parte, occorre concentrarsi sulla sussistenza o meno di un indice di capacità dimostrativa del *match*, in questo caso, seguendo un metodo di comparazione 1:1. Dall'altra, verranno presentate alcune brevi riflessioni circa le corrette modalità di accesso di questa particolare tipologia di *electronic evidence* entro le maglie del processo penale. Con riferimento a questa seconda prospettiva di analisi, essendo il risultato di compatibilità generato automaticamente da un dispositivo digitale, non è prevista una valutazione del calcolo del rapporto fra il grado di similarità e di tipicità rispetto ad una cd. "popolazione di riferimento" (cfr. il capitolo I, § 2.4). Il tratto biometrico grezzo sarà oggetto diretto di comparazione con il modello registrato in precedenza nel dispositivo elettronico, senza il ricorso ad una banca dati di riferimento. Non potendo

[154] Per un approfondimento sulla disciplina della *mobile forensics* v. K. La Regina, *Le indagini su dispositivi digitali*, in AA.VV., *Investigazioni digitali*, (a cura di) M. Iaselli, Giuffrè, Milano, 2020, pp. 27 e ss.
[155] Cfr. il capitolo I, § 2.4.
[156]Si rinvia completamente al capitolo II, §§ 1 e ss.
[157] Cfr. L. Marafioti, *Digital evidence e processo penale*, cit., p. 4510.

dunque elaborare un giudizio sulle modalità di funzionamento del software rispetto ad un database di riferimento, l'analisi verterà sul possibile accesso formale di questa particolare prova generata automaticamente.

Orbene, quanto al primo profilo di analisi, si pensi all'esempio, poc'anzi richiamato, di uno *smartphone* ritrovato nel *locus commissi delicti*, nel quale sono registrate le *features* di un'impronta digitale appartenenti ad un soggetto[158]. L'immagine digitalizzata o il *template* memorizzato, cosa dimostra di semanticamente rilevante per l'oggetto di prova? Esso potrebbe essere interpretato negli stessi termini rispetto al rilevamento di un campione grezzo (es. impronta digitale) su di un oggetto?[159] A differenza dei due casi precedenti, in effetti manca un passaggio inferenziale, ossia l'utilizzo di un software predisposto dagli organi inquirenti a fini di comparazione con i dati presenti all'interno di un database di riferimento. Tuttavia, giova rilevare come il *match* eseguito da uno *smartphone* o da un qualsiasi dispositivo IoT scaturisca da un'operazione di apprendimento automatico da parte di algoritmi, quindi, non sempre verificabile nelle sue effettive modalità di funzionamento (cfr. il capitolo II, § 2.2). Oltre a ciò, non è ancora dato sapere se le attività di estrazione, copia, comparazione e trasformazione del dato biometrico presente all'interno di un dispositivo di tal genere potrebbero causare delle alterazioni compatibili con l'applicazione di un accertamento tecnico irripetibile *ex* art. 360 c.p.p.[160], diversamente da quanto accade per le due tipologie precedenti (cfr. *infra* il § successivo).

Rispetto alla seconda prospettiva di analisi, giova chiedersi come organizzare correttamente l'accesso al contesto dibattimentale di questa tipologia di *electronic evidence*. La dottrina, riferendosi al più esteso ambito della cd. *automated evidence* (cfr. il capitolo II, § 2)[161], ha fatto ricorso all'art. 189 c.p.p., ribadendo che la *ratio* della norma consiste proprio nell'«evitare eccessive restrizioni ai fini dell'accertamento della verità, tenuto conto del continuo sviluppo tecnologico che estende le frontiere dell'investigazione, senza mettere in pericolo le garanzie difensive»[162]. La disposizione, come già accennato brevemente *supra*, ha la finalità di assicurare l'opportuna flessibilità del sistema processuale rispetto al progresso scientifico-tecnologico. Come si approfondirà meglio *infra*, allo

[158] Qui il software automatico di riconoscimento è utilizzato per finalità di "verifica" o "autenticazione", pertanto la modalità di comparazione è 1:1 e non 1:N, 1:N+1. Cfr. il capitolo I, § 2.4.

[159] Giova ricordare che è stato dimostrato scientificamente che è possibile eseguire il procedimento inverso di trasformazione dal modello elettronico biometrico alle caratteristiche del campione biologico grezzo originario. Cfr. il capitolo I, § 2.2.

[160] Come già visto *supra* al capitolo II § 1.3.1, l'orientamento giurisprudenziale maggioritario in tema di estrazione e copia di un dato digitale, ritiene che tali attività rientrino tra gli accertamenti tecnici ripetibili disciplinati dall'art. 354 c.p.p. La comparazione delle impronte digitali prelevate con quelle già in possesso della polizia giudiziaria non richiede poi particolari cognizioni tecnico-scientifiche, risolvendosi in un mero accertamento di dati obiettivi ai sensi dell'art. 354 cod. proc. pen., il cui svolgimento non postula il rispetto delle formalità prescritte dall'art. 360 cod. proc. pen. Cfr. *ex multis*, Cass. pen., Sez. V, 17.3.2004, n. 23319 in *CEDCass* n. 228864. Manca la verifica sulla ripetibilità o meno del secondo passaggio, ossia quello avente ad oggetto il procedimento che permette di risalire dal *template* alla struttura completa del campione biologico grezzo originario.

[161] Cfr. G. Canzio, *Intelligenza artificiale, algoritmi e giustizia penale*, in *www.sistemapenale.it*, 8.1.2021.

[162] Cfr. *Relazione al progetto preliminare del codice di procedura penale*, p. 60, reperibile all'indirizzo https://www.gazzettaufficiale.it/eli/id/1988/10/24/088A4237/sg (visualizzato in data 21.7.2021).

scopo di garantire l'anticipata conoscenza delle parti circa le precise metodologie che saranno applicate durante l'acquisizione della prova, il giudice dopo aver sentito le parti, provvede all'ammissione con ordinanza, fissando le regole per la corretta applicazione dei metodi e delle procedure tecniche di acquisizione della stessa. Il contraddittorio preventivo fra le parti sulle precise modalità di assunzione della prova rappresenta così «un filtro (…) a maglie ben più strette rispetto a quello previsto dall'art. 190, comma 1, che, ai fini dell'ammissione della prova si limita a selezionare negativamente "solo le prove vietate dalla legge e quelle che manifestamente sono superflue o irrilevanti"»[163]. Resta solo da capire – come si avrà modo di approfondire meglio nei successivi paragrafi – se, posta l'esistenza di questo filtro preventivo, esso possa risultare concretamente efficace per la verifica degli schemi statistico-probabilistici acquisiti con l'ausilio di software informatici e con l'apporto di tecniche di IA sviluppate con finalità del tutto estranee al procedimento penale.

1.3.1. Il trattamento del dato biometrico digitalizzato tra accertamenti tecnici ripetibili in fase di indagini preliminari e prova in dibattimento

Prima di approfondire l'analisi delle varie fasi del procedimento probatorio interessate a garantire l'accesso di un dato biometrico automaticamente generato, si ritiene ragionevole, per completezza, formulare ancora qualche breve riflessione in merito al possibile accesso procedimentale delle prime due tipologie di dato poc'anzi accennate. Si è già detto in precedenza che il *match* fra due dati, ottenuti da un procedimento di digitalizzazione o ricavati da un determinato *frame* di videosorveglianza, non sia da ritenersi sempre un elemento semanticamente così significativo per la ricostruzione di un fatto di reato. L'impiego di software automatizzati appartenenti agli organi inquirenti per il trattamento di queste particolari tipologie di dato biometrico potrebbe rientrare entro le attività tipiche[164] o atipiche di indagine[165], inquadrabili entro i compiti istituzionali necessari della polizia giudiziaria ai sensi degli artt. 55 e 348/349 c.p.p., eseguibili anche in autonomia e prima della comunicazione della *notitia criminis* al p.m., al fine di assicurare le fonti di prova e quant'altro possa servire per la ricerca di ogni elemento utile alla ricostruzione del fatto e all'individuazione del colpevole[166]. Per vero, come già

[163] Cfr. G. Canzio, *Intelligenza artificiale, algoritmi e giustizia penale,* cit.

[164] Le comparazioni automatiche di impronte digitali nel sistema A.F.I.S.- S.S.A (cfr. il capitolo I, § 3.3.1) o del Dna con l'ausilio della relativa banca dati istituita con l. 85/2009 (cfr. il capitolo I, § 3.6.3) costituiscono ormai un'attività abituale di indagine.

[165] È stata così definita in dottrina l'attività di estrazione e comparazione automatica delle *features* dei volti tramite il software S.A.R.I., inquadrabile come «una sorta di filiazione spuria del riconoscimento fotografico autonomamente curato dalla polizia giudiziaria, a sua volta derivato atipico dell'"atto omologo" del mezzo di prova della ricognizione, disciplinato dall'art. 361 c.p.p.». Cfr. R. Lopez, *Riconoscimento facciale tramite software e individuazione del sospettato*, in AA.VV., *Pre-investigazioni*. (*Espedienti e mezzi*), (a cura di) A. Scalfati, Giappichelli, Torino, 2020, pp. 311 e ss.

[166] Con specifico riferimento all'utilizzo del software automatico di riconoscimento facciale, cfr. R. Lopez, Riconoscimento facciale tramite software e individuazione del sospettato, in AA.VV., *Pre-investigazioni (Espedienti e mezzi)*, (a cura di) A. Scalfati, Giappichelli, Torino, 2020, p. 311.

peraltro emerso *supra* nel capitolo I § 2, secondo un principio di proporzionalità e di minore offensività dell'attività, alla polizia giudiziaria è riconosciuta la facoltà di chiedere all'interessato di riferire le proprie generalità ed ogni altra notizia utile ai fini dell'identificazione; in secondo luogo è riconosciuta la possibilità di eseguire, «ove occorra», rilievi dattiloscopici, fotografici e antropometrici, nonché altri accertamenti. Da una parte, la genericità della formula «altri accertamenti» consente l'adeguamento della norma alle innovazioni scientifiche tra le quali potrebbero annoverarsi anche quelle oggetto della presente ricerca; dall'altra, l'espressione costituisce un veicolo per potenziali e molteplici strumenti atipici di indagine, assegnando alla polizia giudiziaria «margini non trascurabili di discrezionalità operativa»[167]. In questi casi, i sistemi automatici di riconoscimento costituiscono un atipico strumento d'ausilio per svolgere una prima "scrematura" tra diversi dati compatibili con quelli appartenenti al soggetto sospettato[168]. In seguito all'intervento del pubblico ministero, l'impiego di questi software al fine di attribuire una determinata direzione alle indagini, costituirebbe invece un'attività rientrante fra gli accertamenti tecnici ripetibili, ai sensi dell'art. 359 c.p.p.

Per conferire al risultato di compatibilità espresso dal software maggiore attendibilità, poi, è talvolta necessario un confronto manuale, fra i due dati oggetto di una precedente comparazione automatizzata, da parte di un operatore esperto[169], il quale applica una metodologia di misurazione manuale, conforme agli standard e alle procedure elaborate dalla comunità scientifica di riferimento, atte a stabilire in che misura due modelli elettronici biometrici appartengano alla stessa persona[170]. In questo modo, il risultato scaturente dal sistema, essendo oggetto di verifica da parte dell'esperto, potrebbe trovare accesso nel processo senza la necessità del ricorso ad un contraddittorio preventivo all'ammissione ai sensi dell'art. 189 c.p.p. (cfr. *supra* il § 1.2). L'analisi morfologica/antropometrica compiuta manualmente dal personale tecnico specializzato delle Forze dell'ordine, infatti, non costituirebbe una "nuova prova scientifica", potendo annoverarsi fra gli strumenti tecnico-scientifici di utilizzo consueto e frutto di una ormai condivisa e consolidata esperienza nell'uso giudiziario.

Ciò posto, come già anticipato poc'anzi (cfr. il § 1.2), anche rispetto a strumenti tecnico-scientifici di usuale presentazione in dibattimento, possono vedersi sopraggiungere nuove formulazioni che li mettono in discussione, fino a renderli a un certo punto problematici. A titolo esemplificativo basti pensare all'analisi morfologica di un volto compiuta manualmente da un operatore esperto e al *match*

---

[167] Cfr. T. Alesci, *Corpo dell'imputato (fonte di prova nel processo penale)*, in *Digesto delle Discipline Penalistiche*, Utet, Milano, 2018, p. 81.

[168] Come visto *supra* al capitolo I § 3.5.1, questo non vale per il riconoscimento vocale che, grazie all'impiego di determinati software, è stato oggetto di valutazione da parte del giudice dibattimentale senza previa verifica di un operatore esperto.

[169] Ai sensi degli artt. 220 e 233 c.p.p. (cfr. *infra* il § 1.3.1). L'uso dell'avverbio "talvolta" si motiva con il fatto che ad oggi gli unici risultati scaturenti da software automatici in uso oggi in Italia che non necessitano di un controllo a posteriori da parte di un operatore specializzato sono quelli di riconoscimento della traccia fonica e del Dna. Questo perché il sistema non calcola solo il grado di similarità fra i due dati ma anche il cd. rapporto di verosimiglianza. Cfr. il capitolo I, § 3.5.1.

[170] Attraverso l'esperimento di una perizia tipica ai sensi dell'art. 220 c.p.p. ovvero di una consulenza tecnica *ex* art. 233 c.p.p.

con un dato tratto biometrico scaturente da un software automatizzato o da dispositivo IoT in grado di generare modelli elettronici automaticamente. Questi ultimi si differenziano dalle prime due categorie poiché, come visto[171], non risultano oggetto di alcuna disciplina, neanche di *soft law*, e non sono ancora basati su protocolli di utilizzo sicuri.

1.3.2. Il procedimento probatorio: l'ammissione del dato generato automaticamente

Tornando al controverso tema avente ad oggetto l'accesso di un risultato di compatibilità fra due dati biometrici generato automaticamente da un oggetto di uso quotidiano, collegato o meno alla rete internet, come prova nel processo, parte della dottrina[172] ritiene che - ad oggi[173] - il punto di partenza normativo possa essere individuato ragionevolmente nell'art. 189 c.p.p. Le caratteristiche intrinseche di questa terza tipologia di dato spingono l'interprete a ragionare intorno alla categoria di prova scientifica «nuova o controversa e di elevata specializzazione»[174], dal momento che si tratta di un risultato scaturente da strumenti automatici, attualmente oggetto di discussione in seno alla loro effettiva validità scientifica e frutto di un'esperienza ancora non consolidata nell'uso giudiziario. L'ipotesi individuabile qui è quella di uno strumento probatorio, già conosciuto nell'esperienza giudiziaria[175], giudicato positivamente o, eventualmente negativamente da parte della comunità scientifica di riferimento rispetto all'idoneità alla ricostruzione del fatto (analisi e comparazione di un dato biometrico grezzo a fini di riconoscimento), rispetto al quale, ad un certo punto, si applichino «nuovi fattori teorici, tecnologici o pratici»[176] che sono in grado di mettere in discussione quei precedenti giudizi[177] (comparazione 1:1 eseguita da un dispositivo IoT).

---

[171] Cfr. il capitolo II, § 1.

[172] Cfr. G. Canzio, *Intelligenza artificiale, algoritmi e giustizia penale*, in *www.sistemapenale.it*, 8.1.2021.

[173] Rimane ferma la preoccupazione sollevata da M. Gialuz, *Premessa*, in *Diritto di Internet Digital Copyright e Data Protection*, 1/2020, p. 6, che, anche con riferimento alle "prove algoritmiche" afferma che «si tratta – è evidente – di una situazione non più sostenibile: non è pensabile che in un ordinamento fondato sul principio di legalità processuale (art. 111, comma 1, Cost.) venga delegato completamente alla fonte giurisprudenziale – con la copertura del *passepartout* dell'art. 189 c.p.p. – il delicatissimo compito di bilanciare le esigenze di repressione dei reati e la tutela dei diritti fondamentali pregiudicati dalle prove tecnologiche».

[174] Cfr. *supra* la nota n. 28.

[175] Per esempio l'analisi e il confronto delle impronte digitali, Dna e tracce foniche.

[176] Cfr. O. Dominioni, *La prova penale scientifica*, cit., p. 208.

[177] L'applicazione di tecniche di intelligenza artificiale sempre più sofisticate poste alla base del funzionamento dei software di riconoscimento e di comparazione dei modelli elettronici sta ponendo dubbi di diversa natura in dottrina, v. *ex multis* G. Canzio, *Intelligenza artificiale, algoritmi e giustizia penale*, in *www.sistemapenale.it*, 8.1.2021, C. Cesari, *L'impatto delle nuove tecnologie sulla giustizia penale - un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1169, F. Palmiotto, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in AA.VV., *Algorithmic Governance and Governance of Algorithms, Legal and Ethical Challenges*, (a cura di) M. Ebers, M. Cantero Gamito, Springer, Berlin, 2020, p. 52, G. Ranaldi, *Processo penale e prova informatica*, cit., p. 19, S. Quattrocolo, *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Revista Italo-Española de Derecho Procesal*, 2019, pp. 2 e ss., M. Daniele, *La prova digitale nel processo penale*, in *Riv. Dir. Proc.*, 2011, p. 288, M. Pittirutti, *Digital evidence e procedimento penale*, Giappichelli, Torino, 2017.

È vero infatti che l'utilizzo nel processo di nuove conoscenze derivanti dal progresso tecnico-scientifico consente talora di ottenere una più accurata ricostruzione dei fatti ma ciò comporta anche l'eventuale insorgere di problematiche connesse al tema dell'ammissibilità e dell'affidabilità della prova scientifica. Di tal guisa, come già visto *supra*, a fronte dell'introduzione di una prova scientifica "nuova", il giudice sarebbe tenuto pertanto ad affrontare tali criticità già in fase di ammissione delle prove. Il vaglio, come noto, avrebbe ad oggetto l'idoneità dello strumento probatorio nell'assicurare l'accertamento del fatto[178], l'eventuale incidenza dello stesso sulla libertà morale della persona[179] e la verifica sulla necessità o meno di procedere con modalità atipiche di assunzione[180]. A questo punto,

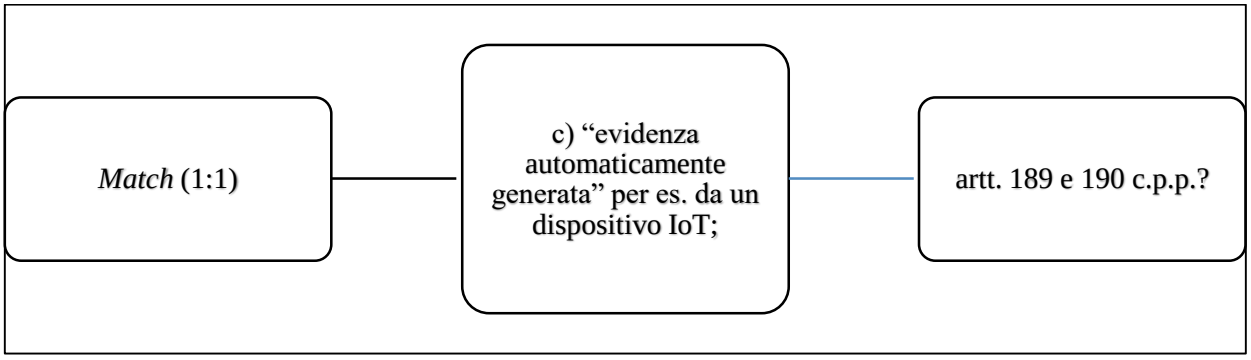
[178] Con riferimento al concetto di idoneità probatoria, giova ricordare il contributo fondamentale derivante dall'elaborazione statunitense (si è già fatto cenno *supra* al § 1.1). Come ormai noto, le connotazioni che concorrono a costituire l'idoneità di uno strumento tecnico-scientifico sono essenzialmente la *validità teorica* del principio e della metodologia dello strumento tecnico che s'intende impiegare nell'operazione probatoria o dei quali l'esperto ha fatto uso fuori dal processo per l'elaborazione dell'oggetto di prova in funzione della sua deposizione nel processo. Qualora la teoria scientifica tradotta in algoritmo non sia convincente, il giudice non può ammettere quest'ultimo nel processo, né impiegarlo a supporto delle scelte decisionali del giudice. Poi, l'*adeguatezza* dello strumento scientifico per la ricostruzione del fatto oggetto di prova; la *controllabilità del corretto uso pratico* in funzione di un'adeguata ricostruzione processuale del fatto; la *qualificazione dell'esperto* che concorre a determinare la validità teorica dello strumento scientifico-tecnico. Infine, un elemento fondamentale per considerare idoneo o meno uno sistema tecnico-scientifico è costituito dalla *comprensibilità dello strumento probatorio*, ossia il dominio delle parti e del giudice sulla fonte di conoscenza giudiziaria. Per vero, con riferimento a quest'ultimo requisito, la dottrina ha evidenziato che «una risorsa tecnico-scientifica che si esibisca con una esasperata sofisticazione tale da sfuggire alla comprensione del giudice e delle parti pur nell'uso più attento e scrupoloso del loro "sapere comune" si sottrae al controllo che tali soggetti, ognuno nel proprio ruolo processuale sono impegnati a esercitare sulla prova nei diversi stadi di sviluppo del fenomeno probatorio: nella fase dell'ammissione, per apprezzarne con cognizione di causa la validità teorica, l'adeguatezza e la verificabilità del suo corretto uso nel caso concreto; nella fase dell'assunzione, per governare l'assunzione della prova in modo che il sapere dell'esperto sia acquisito correttamente e compiutamente, secondo le regole che presiedono alla formazione della conoscenza giudiziaria; nella valutazione per inferire razionalmente dal prodotto ("elemento di prova" dell'operazione probatoria scientifico-tecnica la premessa storica ("risultato di prova") della decisione e per determinare l'efficacia probatoria». O. Dominioni, *La prova penale scientifica*, cit., p. 218. V. su questo punto, in termini piuttosto critici, M. Caianiello, *L'ammissione della prova scientifica nel processo italiano*, in AA.VV., *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Lupária, Wolters Kluwer-Cedam, Milano, 2018, pp. 205 e ss. e F. Caprioli, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008, p. 3529.
Ne consegue che, gli strumenti tecnici che, già in fase di ammissione, non permettono la loro piena comprensione ad opera del giudice e delle parti non possono soddisfare il requisito di idoneità e sono da considerare inammissibili. Qui risiede il confine invalicabile di accesso della prova scientifica al processo. Giova in ogni caso ricordare che trattasi di una verifica (positiva o negativa) che il giudice è chiamato a svolgere sull'ammissione dello strumento scientifico-tecnico, la quale si esprime in termini di "non manifesta inidoneità probatoria". Questo perché, come è stato osservato in dottrina, la soglia di ammissione sarebbe altrimenti troppo elevata e tale da sbarrare l'accesso a prove che, nel progredire della conoscenza giudiziaria, potrebbero rivelarsi utili per una compiuta ricostruzione del fatto. V. sempre O. Dominioni, *La prova penale scientifica*, cit., p. 230.

[179] Quanto al tema della possibile lesività della libertà morale della persona, essa si riferisce sia alla tipologia di strumenti impiegati (per es. la narcoanalisi), sia alle concrete modalità di assunzione probatoria, aventi un possibile impatto sulle condizioni intellettive e volitive della persona. Cfr. F. Cordero, *Procedura penale*, 7 ed., Milano, Giuffrè, 2003, pp. 619 e ss.

[180] Gli altri requisiti di ammissibilità afferiscono alla disciplina contenuta nell'articolo 190 c.p.p., di particolare interesse per le esigenze di economia processuale. Più nel dettaglio, sono prove vietate dalla legge, come tali inammissibili, quelle che incorrono in un divieto normativamente previsto in ordine all'oggetto o al soggetto della prova, ovvero in ordine alla procedura di acquisizione probatoria. La valutazione rimessa al giudice è, in questo caso, vincolata, in quanto di fatto priva di margini di discrezionalità. Quanto al secondo parametro di "manifesta superfluità o irrilevanza delle prove", esso impone al giudice una valutazione estremamente rigorosa nell'esercizio del potere di esclusione delle prove. In questo caso il giudizio riguarda la rilevanza (e pertinenza) della prova, e cioè la sua rispondenza ai parametri indicati dall'art. 187 c.p.p., mentre la superfluità involge una prognosi di più stretta utilità, intendendosi per superflua una prova che sia sovrabbondante o ridondante, e che tenda, cioè, ad acclarare quanto già sia stato accertato o sia comunque accertabile. O. Dominioni, *La prova penale scientifica*, cit., p. 219.

nell'ammettere *ex* art. 189 c.p.p. l'impiego di un nuovo strumento tecnico-scientifico, il giudice, nel contraddittorio delle parti, deve esaminare se occorrano modalità atipiche per la sua assunzione e, in tal caso, fissarle.

Giova domandarsi se il filtro di un contraddittorio preventivo tra le parti sulle modalità irrituali di assunzione della prova, posto come condizione per l'ammissione di una particolare categoria di *electronic evidence* - com'è, in effetti, un dato biometrico automaticamente generato - sia concretamente attuabile. Entro tale contesto, occorre richiamare ancora una volta la Relazione al Progetto preliminare del nuovo codice di procedura penale del 1989, che, con riferimento all'articolo 189 c.p.p., stabilisce come «una norma così articolata possa evitare eccessive restrizioni ai fini dell'accertamento della verità, tenuto conto del continuo sviluppo tecnologico che estende le frontiere dell'investigazione, senza mettere in pericolo le garanzie difensive»[181]. Per garantire, infatti, l'anticipata conoscenza delle parti circa i metodi applicati durante l'accertamento, il giudice dopo aver consultato le stesse sulle modalità di assunzione della prova, provvede all'ammissione con ordinanza e fissa le regole per una corretta applicazione delle procedure tecniche di acquisizione. Il filtro contenuto nell'art. 189 c.p.p. è stato ritenuto maggiormente selettivo rispetto a quello previsto dall'art. 190 comma 1 c.p.p. che, ai fini dell'ammissione della prova, si limita ad escludere solamente «le prove vietate dalla legge e quelle che manifestamente sono superflue o irrilevanti». In questo modo, sarebbe garantito un più significativo rafforzamento del contraddittorio anticipato "per" la prova, ancora prima che "sulla prova"[182].



Schema n. 5

Tuttavia, è stato evidenziato che anche la previsione di un contraddittorio anticipato tra le parti per fissare le modalità di acquisizione di certi strumenti tecnico-scientifici potrebbe ridursi a essere «una

[181] Cfr. *Relazione al Progetto preliminare del nuovo codice di procedura penale del 1989*, p. 60, reperibile all'indirizzo https://www.gazzettaufficiale.it/eli/id/1988/10/24/088A4237/sg (visualizzato in data 29.6.2021).
[182] Cfr. G. Canzio, *Intelligenza artificiale, algoritmi e giustizia penale*, in *www.sistemapenale.it*, 8.1.2021.

questione [puramente] accademica»[183]. Infatti, la costruzione di un contraddittorio dibattimentale "per la prova" riguarda esclusivamente la prova costituenda, diversamente dalla prova scientifica *tout court*, e più in particolare da un risultato di compatibilità generato automaticamente[184], che tende a dislocarsi sempre "prima" ed effettivamente "fuori" dal dibattimento, come prova "precostituita", rispetto alla quale il dibattimento diviene l'"arena" per un contraddittorio solo "sulla prova"[185].

Giova dunque chiedersi se il vaglio preventivo operato dalle parti circa l'idoneità probatoria e la non lesività della libertà morale della persona, per stabilire le precise modalità assuntive della prova, a fronte di un *match* generato automaticamente, risulti di per sé efficace. Il contraddittorio su risultati generati da sistemi computazionali risulta ad oggi concretamente attuabile per le parti? Per vero, s'è già fatto cenno nel capitolo II § 2.2 alla problematica concernente proprio l'inesplicabilità del funzionamento di determinati sistemi automatici. Ne consegue una effettiva impossibilità di falsificazione del risultato elaborato dagli algoritmi. Parte della dottrina ha poi evidenziato anche il diverso pericolo derivante dall'impedimento all'accesso al codice sorgente che li governa, con evidenti ricadute sulla tutela del diritto di difesa (cfr. *infra* il § 2.2)[186]. Trattasi di aspetti in ordine ai quali s'incorre nel rischio che anche le esigenze di tutela del segreto commerciale dello specifico programma informatico utilizzato finiscano per creare una sorta di *legal black hole* (cfr. il capitolo II, § 2.2)[187]. Ebbene, l'opacità e la non percorribilità del preciso funzionamento di taluni meccanismi pregiudicherebbero così il controllo delle parti sui requisiti di idoneità probatoria e di non lesività della libertà morale della persona. La parte, infatti, non può contestare ciò che non conosce e non comprende. Il rischio è che il risultato di compatibilità restituito dal software costituisca una sorta di "*black box result*"[188] ovvero il *match* fra due modelli biometrici potrebbe essere stabilito in un contesto di completa asimmetria informativa (cd. *knowledge impairment*), ponendosi in una posizione del tutto inconciliabile con il rispetto del diritto di difesa, posto che il principio di *equality of arms* implica «*the opportunity of challenging the authenticity of the evidence and of opposing its use*»[189]. La questione è molto controversa e, su di essa, si tornerà ancora (cfr. *infra*, il § 2.2).

---

[183] Cfr. F. Cajani, *Il vaglio dibattimentale della digital evidence*, in *Arch. pen.*, 2013, fasc. 3 anno, LXV, p. 846.

[184] Le fasi di *enrollment* e di registrazione del tratto biometrico grezzo in un dato *repository* sono avvenute necessariamente "prima" del procedimento penale. Cfr. il capitolo I, § 2.2.

[185] Cfr. G. Canzio, *Prova scientifica, ragionamento probatorio e libero convincimento del giudice nel processo penale*, in *Dir. pen. proc*., 2003, p. 1200.

[186] «Invero, lo squilibrio conoscitivo è fenomeno che si riscontra nel processo penale sin da quando, per la soluzione di casi complessi, si è iniziato a fare ricorso a competenze tecniche, scientifiche o artistiche. L'ingresso di saperi specialistici nel processo è difficilmente equilibrato, poiché una delle parti - per lo più quella pubblica - ha accesso alla scienza e alle tecnologie migliori, disponendo di mezzi economici non limitati». S. Quattrocolo, *Equo processo penale e sfide della società algoritmica*, in *Rivista di BioDiritto*, n. 1/2019, p. 138.

[187] Cfr. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *Discrimen*, 15.5.2020, p. 14.

[188] Cfr. il capitolo II, § 2.2.

[189] Cfr. C. Edu, Grande Camera, *Bykov c. Russia*, 10.3.2009, § 90.

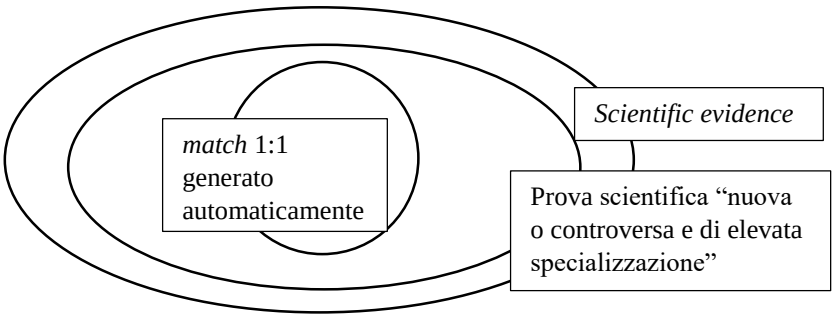
Quanto appena affermato diventa ancora più significativo alla luce della già evidenziata necessità di falsificare la prova scientifica e abbandonare quella che, *ex multis*, è stata definita come la «concezione veritativa» della perizia (cfr. il § 1.1)[190], sottolineando «il ruolo decisivo, che, nell'ambito della dialettica processuale, assume il contraddittorio orale attraverso il quale si verifica, nel dibattimento, l'attendibilità del perito, l'affidabilità del metodo scientifico utilizzato, e la sua corretta applicazione alla concreta fattispecie processuale (…)»[191]. Entro tale scenario, infatti, il dato elaborato digitalmente rischia di risultare attendibile di per sé poiché la verificazione del processo che ha generato quel determinato risultato è troppo complessa per via del ricorso a forme più o meno sofisticate di intelligenza artificiale.

Ciò posto, una problematica strettamente connessa alla comprensione concreta del funzionamento di un sistema digitale destinato ad un uso per lo più commerciale è costituita, poi, dalla possibilità effettiva di vagliare l'affidabilità dell'algoritmo, ossia della possibilità di "accettare" dei risultati basati su generalizzazioni statistiche. L'uso di sistemi automatici di riconoscimento, infatti, può generare rischi di "falsi positivi" o "falsi negativi" (cfr. il capitolo I, § 2.5) e l'accuratezza di un dato generato da un processo computazionale dovrebbe essere sempre oggetto di una puntuale valutazione peritale, nonché essere discussa in contraddittorio nella sua fondatezza empirica, a pena di un'evidente violazione del diritto di difesa[192]. Quanto appena rilevato evoca rischi analoghi a quelli a cui risulta esposta la prova digitale. Tuttavia, rispetto a software automatizzati di riconoscimento, è bene tenere sempre in mente i diversi profili e livelli di complessità cui sono esposti: quello della scienza biometrica, commistione di discipline diverse (cfr. il capitolo I), quello della natura "digitale" dei dati trattati (cfr. il capitolo II), quello concernente l'impiego di processi automatizzati per giungere ad un risultato di compatibilità o meno fra due dati (cfr. il capitolo II, § 2) e quello della validità scientifica della teoria su cui essi si basano[193]. Tutti aspetti che divengono quasi completamente insuperabili qualora «il modello computazionale si basi su meccanismi di autoapprendimento, che portano il software a ricavare le regole [..] non da un diagramma ad albero impostato dall'esperto, ma dall'immagazzinamento di grandi quantità di dati che gli vengono somministrati», dal momento che «lo stesso *designer* non è in grado di spiegare compiutamente e, quindi, di giustificare gli *output* del modello stesso»[194]. Ma come si è opportunamente rilevato, anche qualora «il *reverse engeneering* sia

[190] Cfr. Manes, *L'oracolo algoritmico e la giustizia penale*, cit., p. 15.
[191] Cfr. Cass. pen., S.U., 28.1.2019, n. 14426 in *CED Cass* n. 275112.
[192] Cfr. C. Edu, Grande Camera, *Bykov c. Russia*, 10.3.2009, cit. 90.
[193] Cfr. S. Quattrocolo, *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, in *Cass. pen*., 4/2019, p. 1752.
[194] Cfr. S. Quattrocolo, *Quesiti nuovi e soluzioni antiche?* cit., p. 16.

possibile, la comprensione del modello rimane questione limitata ai soli esperti, con esclusione degli effettivi destinatari della "decisione automatizzata"»[195].

Sembra dunque che già nella fase di ammissione, questa tipologia particolare di *electronic evidence*, sfuggendo il suo funzionamento intrinseco alla comprensione del giudice e delle parti, sollevi diverse criticità[196]. Vien spontaneo però domandarsi cosa potrebbe accadere qualora il giudice determini in ogni caso l'ammissione di un siffatto tipo di evidenza[197].



Schema n. 6

1.3.3. L'assunzione

Sebbene si ritenga che, già in fase di ammissione, l'evidenza biometrica generata automaticamente difficilmente potrebbe soddisfare il requisito di idoneità probatoria, vale la pena formulare alcune riflessioni circa l'eventualità in cui il giudice proceda alla sua assunzione. Trattasi di una fase assai delicata, dal momento che, precedendo l'esercizio della funzione valutativa, ogni momento dell'assunzione probatoria risulta in grado di segnare una traccia indelebile nella convinzione del giudice circa l'attendibilità della prova. In altre parole, l'esercizio della funzione valutativa, a seguito dell'esaurirsi dell'istruzione probatoria, risulta intuitivamente influenzata dall'attività di assunzione, le cui specifiche modalità hanno la funzione di predisporre una corretta percezione della relazione tra

[195] Cfr. S. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *www.lalegislazionepenale.it*, 18.12.2018.

[196] Cfr. O. Dominioni, *La prova penale scientifica*, cit., p. 219.

[197] Giova ricordare che, aldilà della sussistenza dei diversi requisiti poc'anzi richiamati, nel caso in cui il provvedimento di ammissione abbia erroneamente stabilito l'insussistenza di uno o entrambi i requisiti della norma, si ricadrebbe nella disposizione contenuta nell'art. 178 c. 1, lett. *b)* e *c)* c.p.p., in quanto essa richiama il diritto delle parti ad intervenire nel procedimento. Ne consegue un dovere da parte del giudice di ammettere le prove richieste ove ne ricorrano i presupposti di ammissibilità. L'inosservanza di questi costituisce causa di nullità sottoposta al regime intermedio dell'art. 180 c.p.p. Per vero, nel caso opposto, qualora il giudice abbia compiuto in fase di ammissione un giudizio errato in ordine ai parametri per esso assegnati al giudice dall'art. 189 c.p.p., non risulta chiaro quale sia il rimedio in termini di invalidità. Il suggerimento della dottrina è quello di demandare la questione alla fase di valutazione, pur nel contesto di «un malgoverno della nuova prova scientifica e con ogni possibile danno per la corretta formazione probatoria». O. Dominioni, *La prova penale scientifica*, cit., p. 280.

"fatto e valore". Più nel dettaglio, tale fase è finalizzata a fornire gli ulteriori elementi «per una diagnosi conclusiva» rispetto al giudizio formulato in fase di ammissione. Peraltro, in assenza di un'espressa previsione normativa, la dottrina non ha escluso che, anche in una fase piuttosto avanzata come quella di assunzione della prova, il giudice possa escluderla, sebbene sia stata precedentemente ammessa, qualora risulti mancante il requisito dell'idoneità probatoria[198]. Ne consegue che, anche in fase di assunzione, una risorsa scientifico-tecnica che si mostri connotata da un'esasperata sofisticazione scientifica tale da sfuggire alla comprensione del giudice e delle parti, sottraendosi al controllo di tali soggetti, possa essere revocata con ordinanza dal giudice. E ancora. Si ponga anche l'ulteriore ipotesi in cui il *match* generato automaticamente sia assunto come prova nel processo con le modalità stabilite precedentemente con il provvedimento di ammissione ovvero modificate eventualmente *in itinere* con un'ordinanza successiva. Orbene, in tal caso, qualora fossero violati i divieti imposti dal giudice in fase di assunzione, parte della dottrina sostiene che, muovendo da un'interpretazione sistematica dell'art. 191 c. 1 c.p.p.[199], si debba estendere la portata dell'inutilizzabilità non solo ai divieti *ex lege* ma anche *ex judice*. Nel caso in cui poi non siano state osservate le prescrizioni giudiziali stabilite ai sensi dell'art. 189 ult. parte c.p.p., la dottrina individua in via ermeneutica il riferimento normativo nell'art. 178 c.p.p.[200]: nel caso in cui non siano ottemperate le prescrizioni riconducibili alle lettere *b)* e *c)* della norma l'operazione probatoria sarebbe nulla e in quanto tale l'evidenza non risulterebbe fruibile per la decisione.

1.3.4. La valutazione

Sebbene si ritenga, come già sottolineato poc'anzi, che un siffatto genere di prova potrebbe incontrare delle difficoltà di accesso già nelle fasi iniziali dell'*iter* procedimentale probatorio, giova comunque analizzare, seppur per brevi cenni, l'ultimo momento di valutazione. Come noto, questo costituisce lo snodo più insidioso per l'introduzione della prova scientifica in ragione della paradossale insipienza in capo al giudice posto di fronte ad un accertamento di tipo tecnico-scientifico: questa tipologia di prova infatti vede il giudice fruitore di un sapere che gli è di fatto del tutto estraneo[201]. Nonostante ciò, si pretende che sia lo stesso giudice a valutare il risultato di prova e nel compiere tale

[198] Così, O. Dominioni, *La prova penale scientifica*, cit., p. 287.
[199] Cfr. O. Dominioni, *La prova penale scientifica*, cit., pp. 293 e ss.
[200] Cfr. O. Dominioni, *La prova penale scientifica*, cit., p. 295.
[201] Cfr. P. Tonini, C. Conti, *Il diritto delle prove penali*, Giuffrè, Milano, pp. 371 e ss., O. Dominioni, *La prova penale scientifica*, cit., pp. 298 e ss., G. Carlizzi, *La valutazione della prova scientifica*, Giuffrè, Milano, 2019, pp. 2 e ss., J. Nieva Fenoll, *Intelligenza artificiale e processo*, (trad. a cura di) P. Comoglio, Giappichelli, Torino, 2019, p. 83, M. Cecchi, *Il giudice dinanzi alla prova scientifica*, in *Arch. Pen*. 2022, n. 1, pp. 1-11.

impresa, come già accennato *supra*[202], deve evitare essenzialmente due rischi: da una parte, non può scegliere arbitrariamente la teoria prevalente sostituendosi agli esperti, dall'altra non può appiattirsi sulla ricostruzione dell'esperto senza valutarla criticamente. In altre parole, «il giudice è soggetto alla verità scientifica, non a qualsivoglia esito peritale; pertanto, la giurisdizione non può che rimanere imprescindibile garanzia della qualità del giudizio, ossia dell'attendibilità della prova scientifica»[203]. In tal senso, è fondamentale che il giudice spieghi perché le prove acquisite nel corso del processo eliminino ogni ragionevole dubbio sulla ricostruzione dell'accusa (cfr. *infra* il § successivo). Come noto, il rispetto del principio del libero convincimento del giudice è verificabile dalla solidità della sentenza, la quale assume tale qualità in quanto la motivazione risulti convincente[204]. In questo modo, tutte le prove risultano ugualmente autorevoli senza che possa essere attribuito un *quid pluris* alla prova scientifica a pena di un ritorno alla prova legale[205]. Ciò che si chiede al giudice, come già evidenziato *supra*[206], non è certamente il raggiungimento compiuto delle conoscenze che possiede l'esperto, quanto, piuttosto, che egli sia in grado di valutare la validità teorica «del principio scientifico, del metodo tecnologico, della regola tecnica, dell'apparato tecnico che li applica»[207].

Rimane l'evidente difficoltà nel comprendere un dato scientifico estraneo al proprio bagaglio di conoscenze: tuttavia, l'*iter* logico che si deve percorrere a questo punto del procedimento probatorio è quello di un più profondo vaglio di astratta idoneità della prova, rispetto alla fase di ammissione. A tal proposito, la Corte di cassazione non ha mancato di precisare che «poiché il giudice è portatore di una 'legittima ignoranza' a riguardo delle conoscenze scientifiche, si tratta di valutare l'autorità scientifica dell'esperto che trasferisce nel processo la sua conoscenza della disciplina; ma anche di comprendere, soprattutto nei casi più problematici, se gli enunciati che vengono proposti trovino comune accettazione nella comunità scientifica. Da questo punto di vista, il giudice è effettivamente, nel senso più alto, *peritus peritorum*: custode e garante della scientificità della conoscenza fattuale espressa dal processo»[208]. Peraltro, il merito di aver introdotto una serie di criteri volti a valutare la

[202] Cfr. il § 1.1.

[203] Cfr. F. Giunta, *Questioni scientifiche e prova scientifica tra categoria sostanziale e regole di giudizio*, in *Criminalia*, 2014, p. 564.

[204] «(…) la motivazione quale specchio che riflette il prodotto giudiziario; giustificazione dell'opera, che consente anche di misurarla in termini di qualità e quantità». M. Nobili, *Scenari e trasformazioni del processo penale*, Cedam, Padova, 1998, p. 168.

[205] Cfr. G. F. Ricci, *Nuovi rilievi sul problema della "specificità" della prova giuridica*, in *Riv. trim., dir. proc. civ*., 2000, p. 1154.

[206] Cfr. il § 1.1.

[207] Cfr. O. Dominioni, *La prova penale scientifica*, cit., p. 297.

[208] «Il giudice riceve quella che risulta essere accolta dalla comunità scientifica come la legge esplicativa – si dice ne sia consumatore – e non ha autorità per dare patenti di fondatezza a questa piuttosto che a quella teoria. L'acquisizione della legge che funge da criterio inferenziale non è però acritica; anzi è in questo segmento dell'attività giudiziale che si condensa l'essenza di questa. Non essendo esplorabile in autonomia la valenza intrinseca del sapere introdotto dall'esperto, l'attenzione si sposta sugli indici di attendibilità della teoria». Cass. pen., Sez. IV, 14.3.2017, n. 12175 in *CED Cass* n. 270385. Su questo punto v. *ex multis* R. Angeletti, *Il processo indiziario. Indizio, sospetto e congettura al vaglio della giurisprudenza di legittimità*, Giappichelli, Torino, 2021, pp. 84 e ss.

validità e l'attendibilità delle prove scientifiche deve essere indubbiamente riconosciuto alla già più volte menzionata sentenza *Daubert*, i cui principi sono stati accolti dalla nostra giurisprudenza di legittimità con la sentenza Cozzini[209]. Trattasi di una verifica più approfondita rispetto a quella compiuta in fase di ammissione e, arricchita dalle conoscenze portate dalle parti in sede di istruzione dibattimentale, essa costituisce la premessa del ragionamento probatorio che si riflette sul percorso argomentativo successivo[210].

Il momento che interessa maggiormente ai fini dell'analisi di una delle *quaestiones* emerse all'inizio della trattazione del presente capitolo[211], è rappresentato dalla verifica sulla comprensione della prova da cui consegue, in caso di esito negativo, la non fruibilità della stessa. Come è stato evidenziato in dottrina, «quando il giudice non è in grado di apprezzare l'attendibilità e l'accettabilità della prova scientifica, (…) "si profilano i rischi gravissimi dell'impossibilità di utilizzare tecniche raffinate per l'accertamento dei fatti, perché queste rimangono incomprensibili al giudice poco colto, o di una totale e passiva subordinazione del convincimento del giudice al parere espresso dal consulente tecnico, perché il primo non è in grado di valutare razionalmente l'operato del secondo"»[212]. La Corte di cassazione ha inoltre stabilito che «per valutare l'attendibilità di una teoria occorre esaminare gli studi che la sorreggono. Le basi fattuali sulle quali essi sono condotti. L'ampiezza, la rigorosità, l'oggettività della ricerca. Il grado di sostegno che i fatti accordano alla tesi. La discussione critica che ha accompagnato l'elaborazione dello studio, focalizzata sia sui fatti che mettono in discussione l'ipotesi sia sulle diverse opinioni che nel corso della discussione si sono formate. L'attitudine esplicativa dell'elaborazione teorica»[213]. I criteri *Daubert* sono stati così rielaborati e ampliati: risulta dirimente per il giudice interrogarsi sull'affidabilità della teoria scientifica a fronte non solo della sua concreta attendibilità, ma anche dell'utilità e di un'effettiva fruibilità per l'accertamento del fatto in concreto. Ne consegue che, con riferimento ad un modello biometrico generato automaticamente da un dispositivo di uso commerciale, risulta difficile che un giudice possa operare un effettivo vaglio sull'idoneità di siffatto strumento probatorio.

---

[209] Cfr. *supra* la nota n. 40.

[210] Il primo stadio della valutazione che il giudice è tenuto a compiere è quello relativo alla validità della teoria scientifica del singolo elemento di prova assunto nel processo. In seguito, l'organo giudicante è tenuto a verificare l'adeguatezza dello strumento tecnico-scientifico, e se sia stato fatto un corretto uso dello stesso, sarà necessario altresì prendere in considerazione gli eventuali errori metodologici circa l'astratta idoneità esplicativa ai fini dell'accertamento del fatto, mediante l'uso di tali strumenti. Allo stesso modo, l'adeguatezza logica (*fit*, nel lessico statunitense) va sancita non più come "possibile" ma come "certa". Poi, la correttezza dell'uso pratico dello strumento da parte dell'esperto e la completezza della prova, ossia la formulazione da parte dell'operatore di conclusioni effettivamente utili ai fini della ricostruzione del fatto, tenendo in considerazione l'intero insieme di dati rilevanti. Cfr. C. Brusco, *Il vizio di motivazione nella valutazione della prova scientifica*, in *Dir. pen. proc*., 2004, 14, p. 1414.

[211] Cfr. *supra* il § 1.1.

[212] Cfr. O. Dominioni, *La prova penale scientifica*, cit., p. 304 con la citazione di A. Mittone, *Libero convincimento e sapere scientifico: riflessioni sulla perizia nel processo penale*, in *Quest. giust*., 1983, p. 576.

[213] Cfr. Cass. pen., 17.9.2010, n. 43786 in *CED Cass* n. 248943 Cozzini, cit.

L'imperscrutabilità del *match* scaturente automaticamente da un software, seppur costituisca il risultato di un procedimento di comparazione 1:1, e quindi per certi versi, considerato tecnicamente anche più attendibile di un confronto 1:N, 1:N+1[214], condiziona il controllo su tutti i fattori di "idoneità alla ricostruzione del fatto" poc'anzi richiamati e non permette di riscontrare fraintendimenti o sopravvalutazioni rispetto all'attendibilità del risultato di prova. Si pensi, a titolo esemplificativo, al controllo sul corretto uso pratico dello strumento tecnico scientifico (quale fattore dell'idoneità probatoria), rispetto ad un'evidenza algoritmica: in che modo sarà possibile per il giudice comprendere il funzionamento e intuire, senza l'ausilio costante di un esperto, il possibile margine di errore? Errore, peraltro, che può derivare tanto dall'utilizzo di una determinata metodica, quanto dal mancato rispetto di standard o procedure tesi a limitare quanto più possibile una soluzione errata (es. falsi positivi e falsi negativi, cfr. il capitolo I § 2.5). Il giudice, al fine di verificare eventuali margini di errore derivanti dall'imperfezione della tecnica utilizzata, ovvero dalla natura dell'accertamento, o ancora, da contaminazioni esterne ed esercitare un concreto controllo sulla validità della teoria alla base del *match*, dovrà prima di tutto comprendere il funzionamento intrinseco dello strumento probatorio[215]. Tale ultimo aspetto risulta il più critico nel momento in cui «il modello computazionale si basi su meccanismi di autoapprendimento, che portano il software a ricavare le regole [..] non da un diagramma ad albero impostato dall'esperto, ma dall'immagazzinamento di grandi quantità di dati che gli vengono somministrati», dal momento che «lo stesso *designer* non è in grado di spiegare compiutamente e, quindi, di giustificare gli *output* del modello stesso»[216]. E ribadendo quanto già espresso *supra* (cfr. il § 1.3.2), anche qualora «il *reverse engeneering* sia possibile, la comprensione del modello rimane questione limitata ai soli esperti, con esclusione degli effettivi destinatari della "decisione automatizzata"»[217].

1.3.5. La decisione sul modello elettronico biometrico

Una volta analizzato l'apporto che può essere conferito dalle diverse tipologie di dati biometrici digitali all'istruzione dibattimentale, è ora opportuno concentrarsi, seppur per brevi cenni, sulla fase decisoria, al fine di presentare alcune delle *quaestiones* che il giudice è chiamato ad affrontare, con riferimento ad un risultato scaturente direttamente da un software automatico di riconoscimento, senza l'intermediazione di una verifica da parte di un operatore esperto, nella redazione del tessuto

[214] Cfr. il capitolo I, § 2.4.
[215] Cfr. C. Brusco, *Scienza e processo penale: brevi appunti sulla valutazione della prova scientifica*, cit., pp. 61 e ss.
[216] Cfr. S. Quattrocolo, *Quesiti nuovi e soluzioni antiche?* cit., p. 16.
[217] Cfr. S. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *www.lalegislazionepenale.it*, 18.12.2018.

motivazionale. Ad oggi, l'ipotesi di un accesso come prova, in dibattimento, di alcune di queste particolari categorie di *electronic evidence* risulta, per tutti i motivi espressi finora, alquanto controversa[218]. È bene infatti chiarire sin da subito che l'analisi che seguirà percorrerà un sentiero principalmente astratto, faticosamente praticabile allo stato attuale - ma non certo impossibile - se si considerano gli indiscutibili progressi raggiunti in campo scientifico. Pur con le dovute cautele, aventi ad oggetto la mancanza di una specifica "*biometric chain of custody*" e, di conseguenza, di un controllo sistematico esercitato sull'impiego di determinati software automatici da parte della polizia giudiziaria, rimane fermo un loro utilizzo nelle fasi iniziali del procedimento, al fine di orientare le indagini e restringere la ricerca dei sospettati.

Orbene, anche ponendo l'eventualità di una loro ammissione in dibattimento si tratterebbe di verificare a questo punto l'affidabilità del contributo algoritmico e motivarne la sua rilevanza rispetto all'oggetto di prova (v. *supra* il § 1.1.1). Per vero, anche rispetto al passaggio dalla valutazione probatoria alla decisione, sarà necessario sempre tenere in considerazione le distinzioni operate in ordine alle diverse tipologie di modelli biometrici poc'anzi richiamate. Infatti, con riferimento alle prime due tipologie, il risultato probatorio sarà quello proveniente dal controllo "manuale", esercitato - quasi sempre[219] - dall'operatore esperto sulla correttezza del risultato di compatibilità o meno fra due dati. Rispetto a questi, dunque, non si porrebbero particolari problematiche pratiche. Infatti, proprio la verifica forense compiuta dall'operatore specializzato è in grado di confermare o quantomeno confutare il risultato scaturente da un software automatizzato di riconoscimento, anche non potendone spiegare l'effettivo funzionamento per le ragioni esposte *supra* (cfr. il capitolo II, § 2.2).

Il limite di una comparazione con un'evidenza generata automaticamente da un dispositivo di uso commerciale, invece, consiste nel fatto che essa, non solo non sia specificamente disciplinata dalla legge, ma anche non sia basata su protocolli sicuri, provenendo da oggetti di uso quotidiano collegati alla rete internet. A ciò si aggiunga la difficoltà di accesso e il carattere di totale opacità del funzionamento degli algoritmi alla base dei software automatici di riconoscimento (caratterizzante, peraltro, anche i sistemi che richiedono una verifica a posteriori dell'operatore), che rende pressoché impossibile la formulazione di un giudizio sul risultato della sua elaborazione (cfr. il capitolo II, § 2.2). In questo senso, «*there is little space for human intuition in the appreciation of the reliability of this kind of evidence (...) the explanation, the justification of a verdict of un/reliability is traditionally*

[218] Ci si riferisce in particolare al *match* generato automaticamente.

[219] Sono esclusi i riconoscimenti automatici del parlatore e del Dna che, per prassi, non necessitano sempre di un controllo obbligatorio da parte di un operatore esperto. In entrambi i casi, l'utilizzo di un software automatico è inteso come qualsiasi altro strumento tecnico utilizzabile dal perito nell'espletamento dell'accertamento e, quindi, suscettibile di un suo controllo diretto sul corretto funzionamento durante il suo utilizzo.

based on ordinary human prudence, that seldom can be applied to a computational verification»[220]. Proprio con riferimento all'ultima tipologia di dato, pertanto, come sottolineato in dottrina, potrebbe presentarsi il rischio che «il loro ingresso nel processo penale si accompagni ad una autosufficienza euristica discendente dal grado più o meno elevato di condivisione sociale dei risultati della tecnologia e dell'accettazione della sua ineludibile pervasività»[221]. D'altra parte, nonostante le evidenti problematiche di accesso pratico in dibattimento di quest'ultima tipologia di modello elettronico biometrico, di fronte all'utilizzo dell'IA e degli algoritmi in ambito penale non occorre porsi con un atteggiamento di chiusura radicale. Come è stato sottolineato in dottrina, sarebbe «irragionevole – oltre che antistorico – rinunciare alle componenti positive che lo sviluppo tecnologico offre al sistema penale»[222].

Così, con riferimento al trattamento del dato biometrico digitalizzato in senso lato, è stato assegnato, pur con le dovute cautele rispetto a risultati computazionali generati automaticamente e volendo sempre ragionare caso per caso, il valore di prova indiziaria, bisognoso di essere corroborato da altri elementi di prova in grado di «contestualizzare e specificare le "zone d'ombra" tipiche di un'indagine forense di questa tipologia»[223]. Un dato espresso in termini probabilistici – come un *match* o un *non-match* scaturente da un software automatico – può essere certamente utile ai fini dell'accertamento dei fatti oggetto di prova, «ma non è di per sé sufficiente a costituire [l'unica] prova del fatto»[224]. La corrispondenza probabilistica, infatti, necessita, al pari di altre prove, dell'inserimento all'interno di un contesto probatorio più ampio al fine della decisione, dal momento che non permette in nessun caso la ricostruzione dell'evento in ogni suo aspetto.

Tuttavia, all'interno del *genus* "prova indiretta" sono state intraviste due differenti *species*: la prima è la prova indiziaria *ex* art. 192 c.p.p. e la seconda è costituita dall'elemento indiziario singolo, dotato *ex se* di un grado di affidabilità tale da entrare da solo a far parte del patrimonio conoscitivo del giudice[225]. A titolo esemplificativo, si pensi al *match* automatico, riferito ad un unico profilo del Dna

---

[220] Cfr. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, 2020, p. 93.

[221] Cfr. A. Ziroldi, *Intelligenza artificiale e processo penale tra norme, prassi e prospettive*, in *Questione Giustizia*, 18.10.2019.

[222] Cfr. Manes, *L'Oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *Discrimen*, 15.5.2020, p. 19.

[223] Cfr. M. Mendola, *Aspetti informatici delle prove biometriche. Il problema dei "falsi positivi"*, in *Psicologia e Giustizia*, Anno 14, numero 1, Gennaio - Giugno 2013, pp. 20 e ss.

[224] Cfr. M. Taruffo, *La prova dei fatti giuridici. Nozioni generali*, Giuffrè, Milano, 1992, p. 198. Cfr. *ex multis*, Cass. pen., Sez. I, 21.7.2020, n. 21823, *inedita*, ove la Corte sottolinea il valore meramente indiziario di un risultato di compatibilità restituito dal software di riconoscimento facciale S.A.R.I., evidenziando come in quel caso «le immagini poste a base del riconoscimento non erano nitide e non consentivano di riconoscere le fattezze, l'abbigliamento e diversi particolari dell'accoltellatore, per cui non era sostenibile la sussistenza di elementi gravi». Cfr. *infra* il capitolo IV, § 3.2.1.

[225] Cfr. L. Saponaro, *Dall'indizio alla prova indiziaria: il rapporto tra probabilità e certezza*, cit., pp. 124 e ss. Nel senso che ad alcune prove rientranti nella categoria delle prove "indirette" o "critiche" dovrebbe riconoscersi addirittura una «attendibilità superiore rispetto ad altre che pur rientrano in quella delle "dirette" o "rappresentative"», cfr. Cass. pen., Sez. I, 19.6.1992, in *Cass. pen.*, p. 1036.

ricavato da una traccia biologica pura ed eseguito attraverso un software automatico. In questo caso, l'attività di verifica del risultato da parte dell'operatore esperto assumerebbe un valore del tutto "formale": infatti, oltre all'alta riferibilità individualizzante che connota già il dato genetico di per sé, v'è da sottolineare che, anche dal punto di vista tecnico, il calcolo del cd. "rapporto di verosimiglianza" avviene già nella prima fase di estrazione e analisi del profilo del Dna dalla traccia (v. *supra* il § 1.3). Con riferimento al risultato di compatibilità fra i due profili, ne conseguirebbe che «un indizio singolo, ricostruito attraverso il procedimento inferenziale, produc[a] un risultato probatorio indiretto dotato di una tale forza dimostrativa da non necessitare di ulteriori riscontri per assurgere a rango di prova piena»[226]. Anche nel caso del *match* fra due profili del Dna, esso è sì espresso in termini di probabilità di "compatibilità", ma l'efficacia dimostrativa di questa prova sarebbe tale da potersi considerare idonea a entrare *ex se* nel panorama probatorio del giudice dibattimentale.

Insomma, sebbene la categoria di riferimento sia quella della "prova indiretta", il giudice dovrà sempre ragionare caso per caso, tenendo in considerazione la natura dello specifico tratto biometrico considerato, il contesto di acquisizione del dato, la metodologia impiegata nel trattamento, il software impiegato e la descrizione degli algoritmi alla base dello stesso.

Da tempo in dottrina si è riflettuto su:

> «[…] *how well can biometric systems provide evidence beyond a reasonable doubt? The answer depends on the system and specific methods for matching biometrics. However, in most cases, systems will have false positives or false negatives on the order of one in 1.000 to one in 100.000.* [...] *Facial recognition systems work only if the photograph is taken with proper lighting and an especially bland expression on the face. Even then, the error rate for facial-recognition software has proved to be as high as 10% in tests. If that were translated into reality, one person in 10 would need to be pulled aside for extra screening. Fingerprint and iris-recognition technology have significant error rates, too.* [...] *As with any scientific process, biometric readings provide an illusion of infallibility that may be difficult to overcome in court. If a jury sees that a fingerprint was analysed by biometric reader, jurors will likely assume it was read correctly. In Court, what constitutes a reasonable doubt for the reading of a*

[226] Cfr. L. Saponaro, *Dall'indizio alla prova indiziaria: il rapporto tra probabilità e certezza*, cit., p. 124. L'Autrice si riferisce ai campioni biologici puri rinvenuti sul luogo, sull'arma del delitto e/o sul corpo della vittima. In questi casi, l'operazione di estrazione dell'unico profilo di Dna dalla traccia e il successivo passaggio di comparazione tramite software automatizzato permette di conferire al risultato di compatibilità derivante dal *tool* un alto grado di affidabilità. Trattasi di un caso piuttosto raro, solitamente le tracce reperite sulla *scena criminis* costituiscono un *mix* di molteplici profili di Dna differenti. Su questo punto v. anche R. Angeletti, *Il processo indiziario. Indizio, sospetto e congettura al vaglio della giurisprudenza di legittimità*, Giappichelli, Torino, 2021, pp. 234 e ss.

fingerprint? One in a thousand? One in a million? Juries will have to continue adjusting expectations of proof and doubt as biometric measurements change over time»[227].

Pertanto, la ragionevolezza del dubbio circa l'affidabilità di dati biometrici digitalizzati deve essere fondata sia su una metodologia valida e convalidata, sia certamente sul tradizionale libero convincimento del giudice. Com'è stato rilevato in dottrina «*because of its 'black box' nature (…) there is a risk that the judicial role will undergo, in the coming decades, a loss of autonomy in the realm of the appreciation of evidence*»[228]. Si potrebbe ipotizzare, allora, un obbligo di motivazione rafforzata - sulla traccia di quanto già emerso rispetto alla prova scientifica *tout court*, a partire dalla succitata sentenza Cozzini[229], nella giurisprudenza di cassazione - ove una valutazione da parte del giudice fosse in contraddizione con il risultato del sistema algoritmico[230]. In questo modo, sarebbe possibile dimostrare il compimento di un effettivo vaglio da parte del giudice sulla "scientificità" dell'algoritmo, sino ad asserire che, posti gli evidenti limiti di comprensione a fronte di una potenziale *black box*, «esso risponde ai canoni di verificabilità della prova scientifica, avuto riguardo ai principi della controllabilità, della falsificabilità e della verificabilità della teoria posta a fondamento della prova»[231]. In questo modo, come è stato evidenziato con riferimento agli algoritmi di natura predittiva, «l'aggravio dell'attività giudiziale sarebbe, del resto, controbilanciato dal guadagno in punto di affidabilità della stessa, e l'intervento umano corredato da questo peculiare onere motivazionale – al cospetto di una decisione *algorithm based* – potrebbe ridurre la frizione con le garanzie dell'equo processo e con il diritto ad un ricorso effettivo»[232].

Rimane il fatto che senza una tecnologia in grado di spiegare l'effettiva logica delle scatole nere, questa possibilità o rimarrà intraducibile nella pratica o, semplicemente, renderà difficilmente sfruttabili molti di questi sistemi automatizzati, quantomeno a fini probatori.

---

[227] Cfr. W. S. Coats, A. Badgasarian, T. J. Helou, T. Lam, *The Practitioner's Guide to Biometrics*, ABA Publishing, Chicago, pp. 199-200.

[228] Cfr. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, cit., p. 94.

[229] Cfr. *supra* il § 1.1.

[230] Sul tema della motivazione rafforzata, di recente, M. Cecchi, *La "motivazione rafforzata" del provvedimento ovvero la "forza persuasiva superiore"*, in *DPP*, 2019, 1123 ss., C. Conti, *Sicurezza e riservatezza*, in *Dir. Pen. e Processo*, 2019, 11, p. 1572 e M. Cecchi, *Il giudice dinanzi alla prova scientifica*, in *Arch. Pen*. 2022, n. 1, p. 11.

[231] Cfr. Cass. pen., Sez. I, 12.10.2018, n. 52872 in *CED Cass* n. 275058.

[232] Cfr. V. Manes, *L'Oracolo algoritmico e la giustizia penale*, cit., p. 21.

2. Le coordinate costituzionali e i principi fondamentali nel trattamento di sistemi di riconoscimento automatizzati

Una volta inquadrati più specificamente i risultati di *matches* scaturenti da sistemi automatizzati aventi ad oggetto diverse tipologie di dato biometrico digitalizzato entro le categorie tradizionali probatorie, occorre ora soffermarsi sulle garanzie processuali rispetto alle quali l'impatto del trattamento (*processing*) automatizzato dei dati, attraverso modelli computazionali, rischia talvolta di porsi in contrapposizione.

Come accennato *supra*[233], si prenderanno in esame alcuni principi enunciati nella Costituzione italiana e nelle carte internazionali, a garanzia tanto di diritti e libertà attinenti alla sfera personale come, per esempio, la riservatezza - la cui intrusione può essere perpetrata attraverso diversi atti del procedimento penale - quanto, più nel dettaglio, l'insieme delle garanzie processuali comprese nel canone di un "equo" (nella terminologia sovranazionale) e "giusto" (nella terminologia costituzionale interna) processo penale[234].

Trattasi di un'analisi che è stata oggetto di attenzione in ambito europeo solo di recente, nonostante la dottrina statunitense sia da tempo particolarmente sensibile a questi temi, dal momento che le tecniche di riconoscimento in parola hanno trovato subito largo impiego Oltreoceano[235]. Giova ricordare, infatti, che i Paesi europei, avendo forti tradizioni costituzionali alle spalle, hanno cominciato a interrogarsi sulle potenziali lesioni dei diritti fondamentali derivanti dall'impiego di sistemi computazionali nel settore della giustizia penale[236]. Peraltro, come noto, molte fra queste Costituzioni, insieme alla Convenzione europea dei diritti dell'Uomo e alla Carta dei diritti fondamentali dell'Unione europea, sanciscono principi specifici per il processo penale. In questo senso, la Convenzione europea dei diritti dell'uomo, il diritto dell'Unione europea (nell'ambito di sua competenza) e le Costituzioni nazionali rappresentano un valido riparo contro il rischio di potenziali violazioni di diritti fondamentali mediante l'utilizzo di strumenti informatici nei procedimenti penali. Lo scopo dunque dei successivi paragrafi è quello di valutare se, considerate le differenze ontologiche fra le diverse tipologie di dato fino a qui considerate (cfr. il capitolo II, § 1) e i tratti biometrici più rilevanti a fini giudiziari (cfr. il capitolo I, §§ 3 ss.), l'impiego sistematico di software automatizzati di riconoscimento a fini di investigazione e repressione del reato, possa o meno violare, anche

[233] Cfr. il § 1.

[234] La distinzione è posta in evidenza anche in C. Cesari, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, *Porto Alegre*, vol. 5, n. 3, p. 1169.

[235] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit. p. 58 e R. Lopez, *Riconoscimento facciale tramite software e individuazione del sospettato*, cit., p. 302.

[236] Cfr. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*. *A Framework for A European Legal Discussion*, Springer, Cham, 2020, pp. 19 e ss.

potenzialmente, alcuni dei principi sanciti sia a livello costituzionale sia a livello di Convenzione europea dei diritti dell'Uomo. Non sarà, dunque, oggetto di questa parte di ricerca l'impiego di questi software in funzione preventiva e/o di sorveglianza da parte della polizia: la regolamentazione delle attività finalizzate a prevenire la commissione di un reato, infatti, trova collocazione al di fuori del procedimento penale. Anche se, com'è stato osservato, l'attuale tendenza è quella di una «progressiva sfumatura dei confini tra prevenzione e accertamento del reato», o, in altre parole, il diritto penale si sta trasformando lentamente in diritto di polizia[237].

Sin dall'apertura di questo terzo capitolo si è ragionato tenendo conto di due criteri di fondo: *in primis*, sono state formulate alcune riflessioni sull'effettiva capacità semantico-dimostrativa di una probabile corrispondenza fra dati biometrici digitalizzati aventi una provenienza differente, calcolata da software di riconoscimento, rispetto all'oggetto di prova. In secondo luogo, si è ragionato intorno all'affidabilità tecnica di questi strumenti computazionali e all'effettiva capacità delle parti di falsificarla/verificarla. Orbene, nei successivi paragrafi, tali software automatici di riconoscimento saranno analizzati nello spettro di alcuni dei principi fondamentali che regolano l'applicazione della legge, sia nella fase delle indagini preliminari, sia nei passaggi processuali successivi. In particolare, garanzie quali la libertà personale, la parità delle armi e la presunzione di innocenza saranno i parametri impiegati per valutare la legittimità dell'applicazione sistematica di programmi automatizzati di riconoscimento nei procedimenti penali ovvero per esprimere alcune riflessioni sulle possibili condizioni di un loro potenziale utilizzo legittimo. Un'analisi inesatta della *quaestio* potrebbe portare all'adozione di soluzioni computazionali che nel lungo periodo potrebbero rivelarsi contrarie o addirittura lesive di alcune delle garanzie fondamentali per l'individuo.

Al fine di affrontare lo studio dei sistemi di riconoscimento automatici da questa diversa prospettiva e pur sempre con i dovuti distinguo circa i differenti tratti biometrici considerati, si cercherà di operare una suddivisione rispetto alle singole libertà e ai diritti fondamentali coinvolti, con un'analisi delle loro accezioni più tradizionali sino ai contenuti più attuali.

2.1. Il dato biometrico digitalizzato e la libertà personale

L'analisi della progressiva "intrusione" nel corpo dell'individuo per mezzo dell'impiego sistematico di software automatizzati di riconoscimento a fini giudiziari, non può prescindere da una doverosa premessa ermeneutica circa il livello di tutela offerto dalla Carta costituzionale, dalla

[237] Cfr. S. Quattrocolo, *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Rev. Italo-espanola derecho procesal*, 2019, 1, p. 110 e F. Nicolicchia, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Diritto penale contemporaneo*, 2, 2018, p. 2.

Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, nonché dalla Carta dei diritti fondamentali dell'Unione europea. Il processo penale per secoli si è occupato della garanzia dell'*habeas corpus*[238] e solo di recente l'inarrestabile progresso scientifico-tecnologico ha posto i primi dubbi circa i limiti entro i quali l'ordinamento è chiamato a intervenire per delimitare il grado di intrusione sulla fisicità della persona al fine di raccogliere prove[239]. Per vero, nel caso in cui un nuovo *tool* risulti potenzialmente in grado di violare un diritto fondamentale, è necessaria una base normativa di riferimento e un provvedimento del giudice, altrimenti la prova potrebbe considerarsi non ammissibile[240].

È dunque necessario delimitare l'effettiva portata riconosciuta alla libertà personale, al fine di comprendere se vi siano possibili frizioni tra la stessa e il trattamento automatizzato di diversi tratti biometrici a fini giudiziari. L'analisi processual-penalistica della libertà personale non risulta agevolmente separabile da quella costituzionalistica[241]. Invero, com'è stato evidenziato in dottrina «la questione della tutela della libertà personale è certamente ad un crocevia nevralgico dell'intera rete di rapporti tra la tematica dei diritti fondamentali della persona e la tematica del processo»[242]. Per tale ragione, il punto di partenza delle seguenti riflessioni sarà proprio la Carta costituzionale. Invero, il diritto alla libertà personale costituisce il presupposto logico di tutti gli altri diritti di libertà, dal momento che non solo li precede da un punto di vista sistematico, ma li condiziona anche sul piano operativo[243].

In primo luogo, la libertà personale è stata intesa come libertà dalle coercizioni fisiche[244], ossia quelle che comportano un *pati* corporeo da parte di chi le subisce[245]. Gli articoli 13 Cost. e 5 Conv. eur. dir. uomo, rispetto all'"arresto" o alla "detenzione", richiamano nozioni strettamente connesse alla privazione della libertà fisica[246]. Nell'alveo della tutela posta dall'art. 5 Conv. eur. dir. uomo poi

---

[238] Cfr. M. Daniele, *Habeas Corpus. Manipolazioni di una garanzia*, Giappichelli, Torino, 2017, pp. 3 e ss.

[239] Cfr. T. Alesci, *Il corpo umano fonte di prova*, Wolter Kluwer, Milano, 2017, p. 11.

[240] Cfr. AA.VV., *Dimensione tecnologica e prova penale*, (a cura di) L. Luparia, L. Marafioti, G. Paolozzi, Giappichelli, Torino, 2019, p. 48 per una ricostruzione dell'orientamento giurisprudenziale che considera comunque ammissibili le nuove prove tecnologiche lesive dei diritti inviolabili dell'individuo qualora fosse in ogni caso assicurato il rispetto di talune garanzie processuali minime.

[241] Cfr. M. Chiavario, Libertà, III) *Libertà personale* (dir. proc. pen.), in *Enc. giur*. *Treccani*, Roma, 1993, pp. 5 e ss.

[242] Cfr. M. Chiavario, *Processo e garanzie della persona, II, Le garanzie fondamentali*, Giuffrè, Milano, 1984, p. 299.

[243] Cfr. V. Grevi, voce *Libertà personale dell'imputato*, in *Enc. Dir.*, vol. XXIV, Milano Giuffrè, 1974, p. 316, V. Grevi, *Libertà personale dell'imputato e Costituzione*, Giuffrè, Milano, 1976, pp. 1 e ss., AA.VV., *La libertà personale dell'imputato. Verso il nuovo processo penale*, (a cura di) V. Grevi, Cedam, Padova, 1989, T. Alesci, *Il corpo umano fonte di prova*, cit., p. 11.

[244] Cfr. C. Cost., 23.6.1956, n. 2, in *GiC*, 1956, pp. 561 e ss.

[245] Cfr. G. Amato, *Commento all'art. 13 Cost*., in AA.VV., *Commentario alla Costituzione*, (a cura di) G. Branca, Bologna, 1977, pp. 44 e ss., V. Di Nicola, *La libertà personale dell'imputato tra regole smesse, disciplina attuale e sistema futuro*, Boccia, Salerno, 1989, p. 11 e ss., F. Carnelutti, *Principi del processo penale*, Morano, Napoli, 1960, pp. 175 e ss., C. Bonzano, *Gli accertamenti medici coattivi*, Wolters Kluwer, Milano, 2017, p. 61.

[246] Il testo dell'articolo 13 Cost. è reperibile all'indirizzo https://www.senato.it/1025?articolo_numero_articolo=13&sezione=120 (visualizzato in data 10.9.2021). Il testo dell'art. 5 della Convenzione europea dei diritti dell'uomo è reperibile all'indirizzo https://www.echr.coe.int/documents/convention_ita.pdf.

non rientrerebbero «tutte quelle misure che non comportano una "privazione" della libertà personale, ma una mera limitazione della stessa, quali, ad esempio, il divieto di espatrio e tutte le altre misure prescrittive nel nostro ordinamento»[247].

Una seconda interpretazione, invece, identifica la libertà personale nella disponibilità non solo fisica ma anche psichica o morale di sé stessi[248]. Più nel dettaglio, la Corte costituzionale in alcune decisioni si è orientata a favore di un'estensione del diritto di libertà personale al di là di ogni forma di coazione fisica, per ricomprendervi qualsiasi provvedimento che «provochi una menomazione o mortificazione della dignità o del prestigio della persona»[249].

La Corte di cassazione, nell'affrontare successivamente la tematica in esame, pur non negando una qualificazione del concetto di libertà personale conforme alla sua concezione più ristretta di disponibilità della propria persona fisica, ha ritenuto di condividere una lettura più ampia[250]. La Corte costituzionale si è spinta oltre, escludendo uno specifico ambito applicativo dall'esegesi dell'art. 13 Cost. Secondo tale indirizzo interpretativo della Consulta, infatti, gli atti che incidono solo sull'aspetto esteriore dell'individuo oppure obbligano a limitazioni momentanee, non sarebbero da ricondurre alle garanzie dell'art. 13 Cost.[251]. Per vero, seguendo questo indirizzo ermeneutico l'impiego di alcuni processi automatizzati di riconoscimento non inciderebbe in alcun modo sulla libertà personale, eccetto il caso in cui il rifiuto alla sottoposizione non obblighi a ricorrere all'uso della forza[252]. In altre pronunce, il parametro considerato è stato quello invece della «degradazione giuridica dell'individuo» nel senso di «una menomazione o mortificazione della dignità o del prestigio della persona, tale da poter essere equiparata a quell'assoggettamento all'altrui potere in cui si concreta la violazione dell'*habeas corpus*»[253]. La stessa posizione è stata assunta anche da alcune ricostruzioni dottrinarie che hanno ricondotto questo tipo di degradazione alla violazione della "libertà morale" della

[247] Cfr. P. Spagnolo, *Libertà personale e processo*, in *In onore di Mario Chiavario*, *www.lalegislazionepenale.it*, 19.10.2020, p. 165. Per un approfondimento cfr. anche P. Spagnolo, *Il Tribunale della libertà. Tra normativa nazionale e normativa internazionale*, Giuffrè, Milano, 2008 e M. Pisani, *sub art. 5. Diritto alla libertà e alla sicurezza*, in AA.VV., *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, (a cura di) S. Bartole, B. Conforti, G. Raimondi, Cedam, Padova, 2001, pp. 117 e ss.

[248] Cfr. A. Pace, voce *Libertà personale* (diritto costituzionale), in *Enc. Dir*., Vol. XXIV, Giuffrè, Milano, pp. 287 e ss., P. Felicioni, *La prova del Dna nel procedimento penale. Profili sistematici, dinamiche probatore, suggestioni mediatiche*, Giuffrè, Milano, 2018, pp. 180 e ss. e T. Alesci, *Il corpo umano fonte di prova*, cit., pp. 13 e 18.

[249] Cfr. C. Cost., 30.6.1964, n. 68, *GiC*, 1964, pp. 715 e ss.

[250] Cfr. Cass. pen., S.U., 10.10.1987, n. 8, in *CED Cass* n. 177102.

[251] Cfr. C. Cost., 22.3.1962, n. 30, in *www.cortecostituzionale.it*. Con riferimento ai rilievi fotodattiloscopici disciplinati dall'art. 4 t.u.l.p.s. la Corte ha stabilito che: «(…) i rilievi descrittivi, fotografici ed antropometrici, e sempre i rilievi dattiloscopici (almeno nella forma in cui sono attualmente eseguiti in ogni paese del mondo), non importano menomazione della libertà personale, anche se essi possano talvolta richiedere una momentanea immobilizzazione della persona per descriverne o fotografarne o misurarne gli aspetti nelle parti normalmente esposte all'altrui vista o richiedere una momentanea costrizione tendente alla fissazione delle impronte digitali».

[252] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, p. 82.

[253] Cfr. Corte Cost., 29.5.1995, n. 210, in *www.cortecostituzionale.it*.

persona[254]. Dunque, il concetto di "limitazione della libertà personale" ricomprenderebbe sia la libertà fisica che quella morale e di autodeterminazione[255]. In questo senso, sulla base di quest'ultima accezione, sarebbe possibile ipotizzare che l'impiego di alcune tecniche automatizzate di riconoscimento, considerando quantomeno determinate modalità applicative, sarebbe potenzialmente confliggente con la libertà personale. Queste misure, per il solo fatto di essere applicate ad un soggetto in ragione di un suo particolare comportamento ovvero per la sua presenza in un determinato luogo, potrebbero essere in grado di «produrre una condizione e uno stato psicologico di "assoggettamento" conseguente ad un potere di sorveglianza così penetrante»[256]. Per vero, com'è stato rilevato in dottrina, questo fenomeno potrebbe indurre addirittura le persone a modificare comportamenti o abitudini future per sfuggire a determinate forme di accertamento percepite, talvolta, anche come avvilenti[257].

Oltre a ciò, giova ricordare che nei dispositivi tecnologici di uso comune è ormai riposta molta della nostra vita: essendo tali strumenti divenuti «una vera estensione della nostra mente»[258], è necessario riflettere sull'art. 13 Cost. anche al fine di valorizzare quel diritto all'"*habeas data*"[259], contemporanea conseguenza dell'*habeas corpus*. Non sembra infatti fuori luogo prevedere un'estensione della sfera applicativa della norma summenzionata, rispetto all'impiego di sistemi di riconoscimento biometrico di uso anche commerciale. Talvolta, un accertamento esercitato all'interno di un archivio di un dispositivo informatico può risultare particolarmente intrusivo per la sfera individuale, «da mettere in crisi persino l'inviolabilità della psiche, riconducibile appunto alla stessa tutela di cui all'art. 13 Cost.»[260]. L'accezione più ampia di libertà personale, ossia, come visto poc'anzi, quella che fa riferimento alla libertà morale o di autodeterminazione, non può che conservare il proprio contenuto semantico anche in relazione al contemporaneo utilizzo della tecnologia digitale. Allora, a tal proposito, le parole di Stefano Rodotà risuonano ancora profetiche: «senza una forte tutela del "corpo elettronico", dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo»[261].

Occorre a questo punto domandarsi se l'impiego di processi automatizzati di riconoscimento a scopi identificativi nell'ambito del procedimento penale sia dunque potenzialmente in grado di

[254] Cfr. P. Barile, *Diritti dell'uomo e libertà fondamentali*, Il Mulino, Bologna, 1984, pp. 111 e ss.
[255] Cfr. T. Alesci, *Il corpo umano fonte di prova*, cit., p. 18 e L. Parlato, *Libertà della persona nell'uso delle tecnologie digitali*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*, (a cura di) L. Kalb, Giuffrè, Milano, 2019, p. 216.
[256] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 82.
[257] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 83.
[258] Cfr. M. Gialuz, *Premessa*, in *Diritto di Internet Digital Copyright e Data Protection*, 1/2020, p. 7.
[259] Cfr. S. Rodotà, *Dal soggetto alla persona*, Editoriale Scientifica, Napoli, 2007, pp. 20 e ss., B. Galgani, *Habeas data e garanzie fondamentali*, in *Arch. pen. web*., 2019, p. 1 e L. Luparia, *Privacy, diritti della persona e processo penale*, in *Riv. dir. proc*., 2019, pp. 1464 e ss.
[260] Cfr. L. Parlato, *Libertà della persona nell'uso delle tecnologie digitali*, cit., p. 216.
[261] Cfr. S. Rodotà, *Trasformazioni del corpo*, in *Politica del diritto*, 1, p. 22.

produrre effetti lesivi per la tutela della libertà personale, tenendo conto di entrambe le accezioni sopra riportate. Questo risulta opportuno in un'ottica di una precisa positivizzazione di determinate indagini corporali che ancora oggi non trovano una specifica regolamentazione[262].

2.1.1. Il prelievo coattivo di campioni biologici e la libertà personale: cosa ancora non funziona

Le varie accezioni di libertà personale possono assumere un diverso contenuto semantico a seconda del dato e dello strumento di riconoscimento biometrico considerato. Occorre a questo punto analizzare separatamente alcuni degli strumenti di riconoscimento più rilevanti impiegati a fini giudiziari, al fine di formulare brevi riflessioni circa la potenziale - o meno - lesività del diritto alla libertà personale e, in seguito, di altre garanzie fondamentali.

Con riferimento alla comparazione tramite software di profili genetici, si ritiene che eventuali frizioni con la libertà personale possano verificarsi durante le fasi del trattamento del dato biometrico che precedono il momento del confronto automatizzato. Più nel dettaglio, il prelievo per sua natura è finalizzato «a sottrarre dal corpo umano quel materiale (parte di tessuto o liquido organico) necessario per l'esecuzione delle ricerche o di analisi»[263]. Come visto in precedenza nel capitolo I § 3.6.2, questa operazione può essere compiuta anche coattivamente nei confronti del soggetto che «vi soggiace con la propria persona»[264]. In seguito alla nota sentenza n. 238 del 1996 della Corte Costituzionale[265], è intervenuta la l. 30 giugno 2009, n. 85, al fine di colmare una lacuna normativa nel nostro ordinamento e attuare il Trattato di Prüm, volto al rafforzamento della cooperazione internazionale con lo specifico compito di contrastare il terrorismo, la criminalità transfrontaliera e la migrazione illegale[266]. In seguito all'acquisizione coattiva o meno del campione biologico grezzo, si procede tramite digitalizzazione alla sua conversione in un modello elettronico in vista di una possibile comparazione automatizzata attraverso il software CODIS (*Combined DNA Index System*)[267]. Quest'ultima operazione di per sé non sembrerebbe ledere, nemmeno potenzialmente, il diritto alla libertà personale del soggetto, dal momento che in tale fase del trattamento del dato l'operatore specializzato si limita a comparare tramite software due modelli elettronici, senza di fatto incidere in alcun modo nella sfera

[262] Cfr. T. Alesci, *Il corpo umano fonte di prova*, cit., p. 9.
[263] Cfr. P. Felicioni, *La prova del DNA: profili giuridici*, in AA.VV., *Scienza e processo penale: linee guida per l'acquisizione della prova scientifica*, (a cura di) L. De Cataldo Neuburger, Cedam, Padova, 2010, p. 411.
[264] Cfr. R. Orlandi, G. Pappalardo, *L'indagine genetica nel processo penale germanico: osservazioni su una recente riforma*, in *Dir. pen. proc.*, 1999, p. 764.
[265] Per una ricostruzione sistematica delle ragioni che hanno portato all'introduzione della legge 30 giugno, n. 85, cfr. T. Alesci, *Il corpo umano fonte di prova*, cit., pp. 129 e ss. e L. Scaffardi, *Giustizia genetica e tutela della persona. Uno studio comparato sull'uso (e abuso) delle Banche dati del Dna a fini giudiziari*, Wolters Kluwer, Milano, 2017, pp. 179 e ss.
[266] Si rimanda al capitolo I, § 3.6.2.
[267] Cfr. il capitolo I, §§ 2.2. e 3.6.3.

di libertà personale dell'individuo. Giova allora riprendere brevemente quanto accennato inizialmente nel capitolo I §§ 3.6 e ss. e formulare alcune riflessioni sulle operazioni che precedono immediatamente la fase di analisi e comparazione del dato genetico.

Orbene, la legge n. 85 del 2009 come visto ha posto fine a uno dei più emblematici vuoti normativi esistenti nel nostro codice di procedura penale, introducendo l'art. 224 *bis* c.p.p. rubricato "Provvedimenti del giudice per le perizie che richiedono il compimento di atti idonei ad incidere sulla libertà personale" e l'art. 359 *bis* c.p.p. circa il "prelievo coattivo di campioni biologici su persone viventi". L'innesto di tali norme all'interno del tessuto codicistico ha lasciato intatta la possibilità per la polizia giudiziaria di esperire l'attività di prelievo forzoso nei confronti dell'indagato a fini identificativi, ai sensi dell'articolo 349, comma 2 *bis* c.p.p.[268], sopprimendo, invece, la possibilità di effettuare un prelievo *ex* art. 354, comma 3, ult. periodo c.p.p.[269].

Ciò su cui occorre riflettere ancora in questa sede, aldilà delle considerazioni già formulate in ordine ad alcuni difetti di coordinamento nella normativa introdotta[270], è la permanenza, a più di dieci anni dall'entrata in vigore della riforma, di un'evidente incertezza nell'elenco di atti coattivi che risultano consentiti, nel totale silenzio circa le specifiche modalità esecutive da adottare[271]. Nelle norme summenzionate mancherebbe, in primo luogo, un riferimento alla tipologia di prelievo. Sono infatti stabiliti l'oggetto, ossia i peli, i capelli e la saliva, ovvero la finalità, che consiste nella determinazione del profilo del Dna[272], ma è stata tralasciata la disciplina delle specifiche modalità di prelievo, o meglio, quali esatte operazioni siano consentite sul soggetto al fine di raggiungere l'obiettivo summenzionato[273].

Secondariamente, il quesito più rilevante di tutta la normativa introdotta risiede nella *quaestio* diabolica di che cosa si intenda per «accertamenti medici». L'espressione risulta infatti eccessivamente generica, laddove consente di eseguire operazioni consistenti sia in percezioni visive, sia nella somministrazione di sostanze o nell'introduzione di strumenti all'interno del corpo destinatario del provvedimento del giudice. Rispetto a tale categoria indeterminata e indeterminabile, v'è chi ha avanzato l'ipotesi di «una diagnosi di incostituzionalità della disciplina di riferimento»[274].

---

[268] Comma inserito *ex* art. 9, c. 1, d.l. 27.7.2005, n. 144, conv. in l. 31.7.2005, n. 155 ("*Misure urgenti per il contrasto al terrorismo internazionale*"), in vigore dal 8.8.2005.

[269] Aggiunto *ex* art. 10, c. 4 *ter*, d.l. 27.7.2005, n. 144, conv. in l. 31.7.2005, n. 155 ("*Misure urgenti per il contrasto al terrorismo internazionale*"), in vigore dal 8.8.2005, abrogato *ex* art. 27, l. 30.6.2009, n. 85 ("*Trattato contrasto al terrorismo. Istituzione della banca dati nazionale del Dna*").

[270] Cfr. il capitolo I, §§ 3.6.2 e ss.

[271] Cfr. T. Alesci, *Il corpo umano fonte di prova*, cit., p. 135.

[272] Per un approfondimento sul *Dna fingerprint* v. *ex multis*, L. Scaffardi, *Giustizia genetica e tutela della persona. Uno studio comparato sull'uso (e abuso) della Banche dati del Dna a fini giudiziari*, cit., p. 10.

[273] Cfr. l'art. 5 d.P.R. 87/2016.

[274] Cfr. C. Bonzano, *Gli accertamenti medici coattivi. Legalità e proporzionalità nel regime della prova*, Wolters Kluwer, Milano, 2017, p. 329.

La vaghezza rispetto all'*an* e al *quomodo* contribuisce a rendere opache anche le relative attività. Sfumano di riflesso anche le finalità per le quali è possibile esperire determinati "accertamenti medici", posto che la dicitura "ai fini della determinazione del profilo del Dna" si riferirebbe, per sua collocazione, solamente al prelievo. Ne consegue che vi rientrerebbero così, «tutti gli accertamenti compiuti sul corpo dell'imputato o di un terzo mediante l'impiego della medicina, a prescindere dalla loro finalizzazione alla determinazione dell'impronta genetica»[275].

Insomma, nel caso degli "accertamenti medici", non è possibile conoscere quali siano le esatte operazioni praticabili. Ne consegue un'ingiustificabile incertezza circa le concrete modalità da seguire: come è stato evidenziato, «l'intera opera di tipizzazione viene rimessa non già ad una fonte regolamentare, bensì direttamente al giudice, il quale – nella strutturazione dell'ordinanza – avrà peraltro la necessità di ricorrere a nozioni mediche»[276]. In questo senso la questione concerne una mancanza emblematica, la stessa - in una certa misura - che aveva spinto la Corte costituzionale a dichiarare illegittimo l'art. 224 c.p.p.: la lacuna sulle tipologie di misure restrittive adottabili finisce per infrangere inevitabilmente la prescrizione circa la precisazione «nei soli casi e modi previsti dalla legge» contenuta nell'art. 13 co. 2 Cost.

2.1.2. Riconoscimento facciale e libertà personale

Sebbene l'*automated facial recognition technology* sia interamente oggetto del successivo capitolo IV, si ritiene in ogni caso opportuno anticipare i suoi potenziali profili di attrito con l'esercizio della libertà personale.

In primo luogo, occorre distinguere le due modalità di impiego dei software di riconoscimento facciale: in "*real time*" e in "*post remote*". Nella prima ipotesi, la tecnologia consente l'analisi automatizzata dal vivo di volti ripresi in più flussi video, derivanti da telecamere fisse oppure da dispositivi portatili come i telefoni cellulari. L'utilizzo di tale tecnologia è ad oggi sfruttata per lo più a fini di prevenzione da parte delle autorità di pubblica sicurezza e sta sollevando ampi dibattiti fra studiosi, prestigiose istituzioni scientifiche e associazioni per la tutela dei diritti e delle libertà civili circa la sua effettiva legittimità. I rischi per i diritti fondamentali, infatti, come si approfondirà meglio *infra*[277], sono altissimi.

La questione risulta più complessa qualora tali strumenti siano impiegati dalla polizia in modalità "*post remote*". Vien da domandarsi se l'impiego, durante le operazioni attinenti all'identificazione in

[275] Cfr. M. Gialuz, *Radiologia e accertamenti medici coattivi: il difficile equilibrio tra libertà della persona ed esigenze di prova*, in *Riv. it. dir. proc. pen*., 2/2012, p. 572.
[276] Cfr. C. Bonzano, *Gli accertamenti medici coattivi*, cit., p. 250.
[277] Cfr. il capitolo IV, §§ 3.1 e ss.

senso stretto, di siffatte tecniche di riconoscimento facciale da parte della polizia giudiziaria, possa eventualmente ledere la libertà personale dell'interessato, e in quali termini[278]. Come noto, tali adempimenti costituiscono atti non garantiti con cui le autorità di polizia giudiziaria risalgono alle generalità di una persona fisica già individuata. Qualora non sussista il consenso del destinatario a tali operazioni si rende necessaria l'autorizzazione del p.m. per disporre l'accompagnamento coattivo del soggetto agli uffici di polizia, con la possibilità di trattenerlo fino a dodici ore, ovvero fino a ventiquattro ore nel caso in cui l'identificazione risulti particolarmente complessa per motivi espressamente previsti dalla legge[279]. A tal proposito, la mera sottoposizione a processi automatizzati di riconoscimento facciale, non implicando un intervento coercitivo nei confronti dell'indagato, non sembra giustificare l'estensione della garanzia sopra richiamata, anche se, come prospettato in dottrina, «l'assenza del consenso dell'interessato verrebbe del tutto svuotata della sua valenza oppositiva atta ad innescare il necessario intervento del magistrato»[280]. Parrebbe dunque legittima la costrizione che vede l'interessato a partecipare non attivamente, ma come mero soggetto di un *pati*, come avviene per lo svolgimento di rilievi fotografici o per il prelievo di impronte digitali o materiale organico. In tal senso, l'impiego di strumenti automatizzati di riconoscimento non dovrebbe implicare alcuna compressione della libertà personale, intesa nella sua accezione fisica.

Conseguenze certamente più rilevanti potrebbero sorgere dall'utilizzo nel procedimento penale di tecniche di analisi facciale volte alla ricostruzione della personalità del soggetto, finalizzate ad accertare se stia o meno dicendo la verità[281]. In questo caso potrebbe ricadersi nel divieto prescritto dall'art. 188 c.p.p., dal momento che lo strumento sarebbe potenzialmente in grado di influire sulla capacità di autodeterminazione da parte del soggetto destinatario della misura. Oltre a ciò, in ragione di quanto esposto poc'anzi con riferimento alle diverse tipologie di dato biometrico digitalizzato, si potrebbe altresì dubitare dell'effettiva "idoneità" di tali tecniche alla ricostruzione dei fatti, posto che trattasi di strumenti aventi considerevoli margini di incertezza e di errore, di cui occorre senz'altro tenere conto in fase di ammissibilità della prova scientifica e nel giudizio sulla loro attendibilità[282].

Con riferimento alla libertà personale, intesa nella sua accezione più ampia, comprensiva anche della "libertà morale" della persona, si ritiene utile interrogarsi sui potenziali elementi di frizione rispetto alla sottoposizione a riconoscimento facciale del soggetto. O meglio, ci si chiede se l'impiego

[278] Cfr. l'art. 349, c. 2 c.p.p. «alla identificazione della persona nei cui confronti vengono svolte le indagini può procedersi anche eseguendo, ove occorra, rilievi dattiloscopici, fotografici e antropometrici nonché altri accertamenti».
[279] Cfr. l'art. 349, c. 4 c.p.p. Giova ricordare che l'art. 11 d.l. 21.3.1978, n. 59, convertito con modificazioni dalla legge 18.5.1978, n. 191 prevede misure analoghe per i casi in cui una persona, al di fuori del procedimento penale, rifiuti di fornire le proprie generalità alle forze dell'ordine o queste abbiano indizi sufficienti per ritenere la falsità delle relative dichiarazioni o dei documenti.
[280] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale.*, cit., p. 88.
[281] Per un approfondimento v. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., pp. 38 e ss.
[282] Cfr. *supra* i §§ 1.3.

di questi *tools* possa in qualche modo condizionare la libertà di autodeterminazione. La norma di riferimento anche in questo caso potrebbe essere l'art. 188 c.p.p., il quale prescrive che «non possono essere utilizzati, neppure con il consenso della persona interessata, metodi o tecniche idonei a influire sulla libertà di autodeterminazione o ad alterare la capacità di ricordare e di valutare i fatti»[283]. È fatto dunque divieto di utilizzo di metodi che influiscono in generale sulla consapevolezza e sulla capacità di autodeterminazione del destinatario[284]. Anche in questo senso, allora, sembra potersi escludere che la sottoposizione a riconoscimento facciale avente scopi meramente identificativi implichi una potenziale violazione della libertà morale in quanto la misura sarebbe svuotata di quel rapporto dialogico tipico fra il destinatario come fonte di prova e l'autorità procedente[285]. Tuttavia, come è stato osservato, la mancanza assoluta di una disciplina legislativa di riferimento produce conseguenze potenzialmente significative in termini di tutela della persona[286]. Più nel dettaglio, mettendo a paragone la lacuna giuridica in cui versano i procedimenti automatizzati di riconoscimento facciale con un altro strumento fondamentale a fini identificativi, quale quello che permette la comparazione automatizzata del Dna, si potrebbero porre in luce differenze e analogie che potrebbero costituire ragionevolmente la base per una possibile proposta di regolamentazione. Orbene, come già ampiamente visto nel capitolo I, le due caratteristiche biometriche presentano proprietà e qualità differenti, dall'«irrepetibilità delle caratteristiche genetiche di ognuno, a differenza delle somiglianze nei volti delle persone», all'«immodificabilità dell'architettura genetica di qualsiasi individuo nonostante il passaggio del tempo in contrapposizione al mutare dei tratti somatici», dalla «complessità e la delicatezza delle attività tecnico laboratoriali legate all'analisi del materiale biologico e alla conservazione delle risultanze, rispetto ai processi algoritmici che si svolgono nella dimensione virtuale», all'«alta affidabilità dell'identificazione tramite il Dna, a fronte del tasso di errore insito nel riconoscimento facciale, specie se operato dal vivo»[287]. Ciò nonostante, vi sono anche importanti analogie che connotano i due dati, tra cui si ricorda l'influenza della disciplina statistica applicata. Se già però non sono poche le incertezze interpretative circa le specifiche modalità da seguire per l'esecuzione degli "accertamenti medici"[288], nonostante l'intervenuta riforma del 2009, s'immagini quanto sia necessario estendere le disposizioni normative esistenti con riferimento

[283] Trattasi di una regola operativa valida sia per la formazione della prova tipica che quella atipica. P. Felicioni, *Art. 188*, in AA.VV., *Codice di procedura penale commentato*, (a cura di) A. Giarda, G. Spangher, I, Wolters Kluwer, Milano, 2017, 1875, p. 286.

[284] Cfr. F. Cordero, *Procedura penale*, Giuffrè, Milano, 2012, p. 620 rileva che «tale divieto colpisce qualunque intervento manipolante, grossolano o sottile: ad esempio le veglie coatte, […] fame, sete, luce abbagliante, buio, caldo e freddo, esami estenuanti, messinscene traumatiche […] e minacce, naturalmente […] ovvero esche quali l'impunità o favori offerti sotto banco».

[285] Cfr. P. Felicioni, *Art. 188 c.p.p.*, cit., p. 1875 ss.

[286] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 92.

[287] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., pp. 92 e ss.

[288] Cfr. supra il § 2.1.1.

all'impiego di *tools* automatizzati di riconoscimento facciale, soprattutto laddove consentano un ampio margine di discrezionalità alle forze di polizia giudiziaria sui casi e le modalità applicative.

Insomma, nonostante, le possibili problematiche interpretative e l'evidente difficoltà, o meglio impossibilità, del diritto di cristallizzare l'impiego di tecniche innovative per l'accertamento del fatto, è necessario porsi nell'ottica dell'inserimento nel nostro ordinamento di una disciplina completa che, al pari della l. 85/2009, sia tesa ad assicurare le più ampie forme di tutela e garanzia ai soggetti interessati da questa particolare tipologia di riconoscimento.

2.1.3. Impronte digitali e libertà personale

Si ritiene che, con riferimento alla disciplina dattiloscopica, possa essere adottato lo stesso tipo di approccio adoperato *supra* rispetto al Dna. Le possibili frizioni con la libertà personale, infatti, potrebbero verificarsi non tanto in fase di comparazione automatizzata delle *features* che compongono le impronte digitali tramite software, quanto durante le fasi del trattamento che precedono immediatamente il momento del confronto.

A dire il vero, la Corte costituzionale, in una nota sentenza del 1962[289], ha stabilito che, nonostante i rilievi dattiloscopici costituiscano una misura che implica una coercizione, essi non determinano alcuna violazione della libertà personale. Più nel dettaglio, la Corte ha affermato che gli atti coattivi, intesi come momentanee immobilizzazioni per consentire la misurazione antropometrica o la fissazione delle impronte digitali, «pur avendo per oggetto la persona, riguardano l'aspetto esteriore della persona, la cui sfera di libertà resta integra»[290]. L'orientamento interpretativo è rimasto essenzialmente intatto. Ne consegue che, con riferimento all'ipotesi di acquisizione di un'impronta digitale direttamente dal sospettato, della sua successiva trasformazione in un modello elettronico biometrico e, infine, della sua comparazione automatizzata e verifica manuale, non si pongono particolari *quaestiones*. Giova domandarsi però se questo valga anche rispetto alla terza tipologia di dato biometrico digitalizzato scaturente da dispositivi in grado di generare ed elaborare *match* automaticamente per finalità estranee al procedimento penale, quali assistenti domestici o dispositivi elettronici di rilevamento delle proprie caratteristiche fisiologiche e/o comportamentali. Il dubbio prende spunto da una sentenza della Corte Suprema dei Paesi Bassi avente ad oggetto la legittimità o meno di un'attività coattiva di sblocco biometrico dello *smartphone* sequestrato, appartenente ad un

[289] Cfr. Corte Cost., 27.3.1962, n. 30, in *www.cortecostituzionale.it*. Ci si è soffermati sulla sentenza anche *supra*, al § 2.1.
[290] Cfr. Corte Cost., 27.3.1962, n. 30, cit.

soggetto sospettato, da parte della polizia giudiziaria[291]. In assenza di una cooperazione da parte dell'indagato, la polizia giudiziaria può compiere atti di coercizione fisica in tal senso? Quali garanzie fondamentali ne risultano imprescindibilmente implicate? In quale caso, previsto dalla legge potrebbe rientrare questo tipo di intrusione nella sfera fisica dell'indagato? Rispetto alla protezione della libertà personale, nel codice di procedura penale italiano un caso come questo difficilmente potrebbe rientrare sia nella disposizione contenuta nell'art. 349 co. 2 *bis* c.p.p. sia nell'art. 359 *bis* co. 1 c.p.p., a meno che tale operazione sia ricondotta esegeticamente al *genus* "accertamenti medici", ma, in questo modo, si estenderebbe enormemente il suo significato già di per sé piuttosto generico (cfr. *supra*, il § 2.1.1). Rimane poi il fatto che, come visto poc'anzi, l'orientamento maggioritario della Cassazione ritiene che l'atto coercitivo esercitato per imprimere e registrare le impronte digitali, teso ad un tipo di accertamento "manuale", sia da intendere come una momentanea immobilizzazione, escludendo qualsivoglia violazione dell'integrità fisica della persona. Pertanto, si ritiene, con un certo margine di probabilità, che lo stesso tipo di conclusione potrebbe riguardare anche il caso in cui l'accertamento coinvolga un *automated biometric recognition system*.

Per vero, diverse riflessioni potrebbero, invece, sorgere con riferimento al principio del *nemo tenetur se detegere*, su cui s'intende tornare meglio *infra*, § 2.3.

2.1.4. Impronta fonica e libertà personale

Il riconoscimento automatico o semi-automatico della traccia fonica, generalmente implica una, seppur minima, collaborazione da parte del soggetto destinatario dell'atto. Infatti, al fine di eseguire una perizia (o consulenza tecnica) fonica è necessario che il soggetto ivi sottoposto rilasci un saggio vocale: solo in questo modo l'elaboratore potrà esprimere, sulla base di calcoli matematico-statistici, un giudizio di similarità o dissimilarità avuto riguardo alla voce anonima registrata sui nastri di qualsiasi documento fonografico ovvero di un'intercettazione. Occorre, pertanto, *in primis* reperire il campione di confronto. Anche in questo caso la *quaestio* avente ad oggetto la potenziale violazione o meno del diritto alla libertà personale sembra concernere solo la fase preliminare, avente ad oggetto le procedure acquisitive che superano l'eventuale diniego di cooperazione da parte del riconoscendo. Questo certamente può avere delle implicazioni in termini di rispetto del principio di "*nemo tenetur se detegere*", ma sull'argomento si tornerà meglio *infra*[292].

[291] Hoge Raad, 9.2.2021, n. 19/05471, reperibile su https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2021:202 (visualizzato in data 28.9.2021). Per un approfondimento cfr. A. Pivaty, *Suspects' privilege against self-incrimination not violated when made to unlock smartphone with fingerprint, Dutch Supreme Court rules*, in *Fair Trials*, 19.2.2021.
[292] Cfr. *infra* il § 2.3.

Occorre domandarsi dunque se sia possibile costringere con la forza qualcuno a parlare. Se sì, il rilascio di un saggio fonico può costituire un atto coercibile fisicamente[293]? Si consideri l'ipotesi in cui il campione vocale debba essere acquisito da un soggetto diverso dall'imputato. In questo caso, il terzo costituisce un "ingranaggio" fondamentale ai fini dell'accertamento del fatto, la cui collaborazione si pone come uno «tra i doveri inderogabili [...] che la legge può imporre ai consociati [ossia] quello di concorrere all'accertamento del fatto oggetto del processo penale»[294]. Prendendo come parametro l'interpretazione più estesa dell'art. 13 Cost., ossia la libertà personale non solo da forme di coercizione fisica, ma anche dall'imposizione di doveri rispetto alle "manifestazioni fisiche della personalità", potrebbe verificarsi una possibile intrusione. In tal senso, com'è già stato evidenziato, «l'obbligo di rilasciare un campione vocale indirettamente limita la libertà del soggetto di decidere il proprio comportamento»[295]. Entro la garanzia della libertà morale sarebbe altresì ricompresa la possibilità di conoscere la futura utilizzazione procedimentale o processuale del contenuto informativo acquisito tramite il rilievo compiuto. Ovviamente ciò non è sempre sufficiente per sostenere la sussistenza di una violazione della libertà personale: occorre che si verifichi una vera e propria «degradazione giuridica della personalità morale» del soggetto, ossia «una menomazione o mortificazione della dignità o del prestigio della persona tale da poter essere equiparata a quell'assoggettamento all'altrui potere in cui si concreta la violazione dell'*habeas corpus*»[296]. Risulta difficile, dunque, sostenere un'automatica violazione del diritto, tenuto conto anche del dovere di collaborazione civica per l'accertamento del fatto di reato.

Così, alla luce di queste brevi riflessioni, si concorda con l'orientamento interpretativo dottrinario maggioritario che ritiene che l'imposizione dell'obbligo di cooperare del terzo, mediante il rilascio di un campione fonico, non configuri a prescindere una limitazione all'esercizio della libertà personale, dovendosi sempre considerare le specifiche circostanze del caso concreto.

2.2. Il dato biometrico digitalizzato e la parità delle armi

Parallelamente, occorre riflettere sull'impiego degli *automated biometric recognition systems* nella prospettiva del "giusto processo" e del più specifico ambito del diritto di difesa. Il primo principio che

[293] Anche T. Alesci, *Il corpo umano come fonte di prova*, cit., pp. 102 e ss. si pone lo stesso quesito.
[294] Cfr. P. Felicioni, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Ipsoa, Milano, 2007, p. 31.
[295] Cfr. M. Biral, *L'identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, in *Rivista Italiana di Diritto e Procedura Penale*, fasc.4, 2015, p. 1842.
[296] Cfr. Corte Cost., 31.5.1995, n. 210, Corte Cost., 7.12.1994, n. 419, Corte Cost., 27.3.1962, n. 30 tutte reperibili su *www.cortecostituzionale.it*.

di per sé, come osservato in dottrina[297], più che un concetto costituisce ormai uno "slogan", copre diverse declinazioni delle garanzie processuali. Occorrerà pertanto fare riferimento sia alla Costituzione, sia alla Convenzione europea dei diritti dell'Uomo, entro la quale il diritto ad un giusto processo ha ormai assunto un ruolo centrale (art. 6 Conv. eur. dir. uomo)[298]. Il principio guida che regola questo articolo è l'"equità", interpretata dalla Corte europea dei diritti dell'uomo come una garanzia squisitamente procedurale[299]. L'articolo 111 co. 1 Cost. risulta coerente laddove l'espressione «giusto processo» è stata testualmente utilizzata per indicare il mezzo con cui si attua la giurisdizione[300]. Più nel dettaglio, l'articolo 6 Conv. eur. dir. uomo si compone di tre paragrafi in cui è possibile distinguere tra un insieme di garanzie di contesto e un insieme di principi specificamente riferiti al processo penale[301]. Il § 1 fissa la garanzia dell'indipendenza, dell'imparzialità e della costituzione legislativa del giudice, ma anche la durata ragionevole del processo e, quantomeno come regola, la pubblicità delle udienze. Il § 3 pone invece i cd. "diritti difensivi minimali", tra i quali figurano il diritto alla conoscenza dell'accusa e il diritto alla fruibilità di adeguati tempi e opportunità difensive, il diritto all'autodifesa o all'assistenza tecnica del difensore, il diritto al confronto con i testimoni a carico, nonché l'uguaglianza di trattamento fra testi a carico e testi a discarico e il diritto alle prestazioni gratuite di un interprete in caso di mancata comprensibilità della lingua ufficiale delle udienze. Il § 2, stabilendo il principio di "presunzione di innocenza dell'imputato", si pone come «cerniera»[302] fondamentale fra le due disposizioni[303]. Per vero, l'articolo 111 Cost. ripropone con alcune varianti lo schema dell'art. 6 Conv. eur. dir. uomo. Il secondo comma, facendo riferimento a qualsivoglia tipologia di processo, ne prescrive lo svolgimento «nel contraddittorio fra le parti, in condizioni di parità, davanti ad un giudice terzo e imparziale», e, in conclusione, stabilisce che «la legge ne assicura la ragionevole durata». I commi successivi riguardano esclusivamente il processo penale: come noto, ivi sono contenute una serie di garanzie difensive riservate alla «persona accusata

[297] Cfr. M. Chiavario, *voce "Giusto processo"* (processo penale), in *Enciclopedia giuridica Treccani*, Roma, 2001, p. 1, P. Ferrua, *Il giusto processo*, Zanichelli, Bologna, 2012, p. 1, parla di «modello ideale». Cfr. anche M. Chiavario, *Diritto ad un processo equo*, in AA.VV., *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, (a cura di) S. Bartole, B. Conforti, G. Raimondi, Cedam, Padova, 2001, pp. 154 e ss.

[298] Cfr. A. Cabiale, *I limiti alla prova nella procedura penale europea*, Wolters Kluwer - Cedam, Milano, 2019, pp. 192 e ss., R. E. Kostoris, *Processo penale e paradigmi europei*, Giappichelli, Torino, 2018, pp. 203 e ss. e G. Di Chiara, *Fair Trial e "giusto processo" italiano*, in AA.VV., *I principi europei del processo penale*, (a cura di) A. Gaito, Dike, Roma, 2016, pp. 73 e ss.

[299] Cfr. F. Palmiotto, *Black box on trial: the Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in AA.VV., *Algorithmic Governance and Governance of Algorithms*, (a cura di) M. Ebers, M. Cantero Gamito, Springer, Berlin, 2020, p. 59.

[300] Cfr. M. Chiavario, voce *"Giusto processo"* (processo penale), cit., p. 3.

[301] Cfr. M. Chiavario, *Diritto ad un processo equo*, cit., pp. 154 e ss.

[302] Cfr. M. Chiavario, voce *"Giusto processo"* (processo penale), cit., p. 5.

[303] Posti a completamento delle garanzie del processo penale "giusto" sono gli artt. 2 e 4 del IV Protocollo aventi ad oggetto la tutela del principio del doppio grado di giudizio nei confronti del condannato penalmente e del *ne bis in idem*. L'articolo 3 del Protocollo stabilisce, infine, il diritto a indennizzo per i casi di condanna penale dovuta a errore giudiziario.

di un reato», mentre il comma 4 è dedicato al principio del contraddittorio nella formazione della prova[304], con la precisazione che «la colpevolezza non può essere provata sulla base di dichiarazioni rese da chi, per libera scelta, si è sempre sottratto all'interrogatorio da parte dell'imputato o del suo difensore». Seguono, infine, le garanzie già presenti nel testo originario dell'articolo[305], ossia quelle della motivazione per tutti i provvedimenti giurisdizionali e della ricorribilità per cassazione di tutte le sentenze e di tutti i provvedimenti sulla libertà personale.

Tutte le garanzie richiamate trovano applicazione nei confronti della «persona accusata di un reato»[306]. Tale concetto gode di un'interpretazione autonoma nella giurisprudenza della Corte europea dei diritti dell'Uomo secondo la quale un'ipotesi di accusa esiste «*from the moment that an individual is officially notified by the competent authority of an allegation that he has committed a criminal offence, or from the point at which his situation has been substantially affected by actions taken by the authorities as a result of a suspicion against him*»[307]. Ne consegue che le garanzie del giusto processo debbano trovare piena applicazione durante l'intero procedimento penale, compresa la fase delle indagini preliminari[308]. Pertanto, l'impiego di *tools* automatizzati deve essere compatibile con quanto stabilito nelle disposizioni, sin dalla iniziale fase delle indagini preliminari. Con riferimento all'ambito di utilizzo di questi strumenti a fini investigativi ed, eventualmente, probatori, il canone del contraddittorio e il connesso principio di parità delle armi assumono una certa rilevanza[309]. Nella nota pronuncia *Al-Khawaja e Tahery c. Regno Unito*[310], la Grande Camera ha stabilito che, prima che un imputato possa essere condannato, tutte le prove contro di lui devono essere presentate al suo cospetto in una pubblica udienza, dando la possibilità di presentare delle controprove. Orbene, con riferimento a quest'ultimo aspetto occorre riflettere sul grado di comprensione e falsificabilità di strumenti di riconoscimento automatici basati, ormai nella maggioranza dei casi, su sistemi computazionali che sfruttano tecniche di apprendimento automatico e rispetto ai quali l'accesso ai codici sorgente che governano l'algoritmo risulta solitamente precluso[311]. Le parti sono effettivamente poste nella

[304] Le eccezioni alla regola del contraddittorio sono previste nel quinto comma, ove si demanda alla legge di regolare i casi in cui la formazione della prova non ha luogo nel contraddittorio fra le parti per consenso dell'imputato o per accertata impossibilità di natura oggettiva o per effetto di provata condotta illecita.

[305] Ci si riferisce al periodo precedente alla l. cost. n. 2/1999.

[306] Art. 111 c. 3 Cost. Su questo punto v. M. Chiavario, *Diritto ad un processo equo*, cit., pp. 161 e ss.

[307] Cfr. M. Chiavario, *Diritto ad un processo equo*, cit., p. 162. In particolare v. *Deweer v. Belgium*, 27.2.1980, §§ 42–46, 6903/75; *Eckle v. Germany*, 15.7.1982, § 73, 8130/78; *Ibrahim and Others v. the United Kingdom* [GC], no. 50541/08, 50571/08, 50573/08 e 40351/09, §249, 2016.

[308] Cfr. M. Chiavario, *Diritto ad un processo equo*, cit., pp. 162 e 163.

[309] Cfr. M. Chiavario, *Diritto ad un processo equo*, cit., pp. 222 e ss:

[310] Cfr. *Al-Khawaja e Tahery c. Regno Unito*, 15.12.2011 (ricc. nn. 26766/05 e 22228/06).

[311] Cfr. S. Quattrocolo, *Equo processo penale e sfide della società algoritmica*, cit., p. 138. Sullo stesso tema v. anche S. Quattrocolo, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, Saggi - Focus: innovazione, diritto e tecnologia: temi per il presente e il futuro, pp. 126 e ss., S. Quattrocolo, *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Rev. Italo-espanola derecho procesal*, 2019, 1, pp. 108 e ss., S.

condizione di poter contestare l'attendibilità dei risultati generati dal software? Entro tale scenario, come già accennato in precedenza[312], può crearsi una situazione di effettivo squilibrio conoscitivo tra le parti del processo. Per vero, tale sbilanciamento risulta riscontrabile anche con riferimento alla generale facoltà di introduzione di saperi specialistici nel procedimento, dal momento che la parte pubblica ha solitamente accesso alle tecnologie più avanzate, disponendo peraltro di risorse economiche non limitate. Tuttavia, com'è stato rilevato in dottrina, «la prova algoritmica (…) introduce la forma più estrema di tale squilibrio, poiché il risultato probatorio può essere non criticabile laddove, appunto, l'inaccessibilità del codice sorgente o altre caratteristiche del software non consentano alla parte contro la quale la prova è introdotta nel processo di contestarne l'accuratezza e l'attendibilità»[313]. La *quaestio* ha dunque ad oggetto la protezione del principio di parità delle armi la cui interpretazione, nella giurisprudenza della Corte europea dei diritti dell'uomo, non implica un'automatica identità di facoltà o posizioni di cui le parti debbano sempre fruire[314] ma nella possibilità di presentare le proprie argomentazioni in una condizione non svantaggiosa[315]. O ancora meglio: la parità risiede nella concreta opportunità di contestare o falsificare le allegazioni o le argomentazioni della controparte[316].

In questo senso, è dubbio se, con riferimento all'impiego a fini di indagine o, eventualmente, di prova, di un risultato di compatibilità fra due dati biometrici digitalizzati, generato da un software di riconoscimento, possa intravedersi una potenziale violazione dell'art. 6 Conv. eur. dir. uomo, ovvero dell'art. 111 Cost. A tal proposito, occorre eseguire nuovamente alcune distinzioni rispetto alle diverse tipologie di dato biometrico considerate. Nel caso in cui l'impiego del *tool* avesse una finalità squisitamente procedimentale e fossero considerati dati biometrici, frutto della digitalizzazione di un campione grezzo o di una traccia biologica, ovvero ricavati da un *frame* di un video o da una determinata immagine digitale, non sarebbero riscontrabili particolari problematiche connesse ad una potenziale violazione delle disposizioni richiamate. Per esempio, nel caso del riconoscimento facciale, il software automatico, impiegato in fase investigativa, restituisce un risultato solamente "parziale", in quanto privo del calcolo del cd. "rapporto di verosimiglianza", oggetto di una successiva stima e valutazione da parte di operatori esperti (cfr. il capitolo I, § 3.3.1). Ancora, nel caso di una

Quattrocolo, C. Anglano, M. Canonico, M. Guazzone, *Technical Solutions for Legal Challenges: Equality of Arms in Criminal Proceedings*, in *Global Jurist*, vol. 20, no. 1, 2020, p. 6, C. Casonato, *Intelligenza artificiale e giustizia: potenzialità e rischi*, in *DPCE Online*, v. 44, n. 3, 2020, pp. 3379 e ss., J. Nieva Fenoll, *Intelligenza artificiale e processo*, (trad. a cura di) P. Comoglio, Giappichelli, Torino, 2019, p. 130.

[312] Cfr. *supra* il § 1.1.1.

[313] Cfr. S. Quattrocolo, *Equo processo penale e sfide della società algoritmica*, cit., p. 139.

[314] Cfr. P. Van Dijk, G. J. H. Van Hoof, T*heory and Practice of the European Convention on Human Rights*, 5rd ed., Intersentia, Cambridge, 2018, pp. 562 e ss.

[315] Cfr. C. eur., 7.6.2001, *Kress c. Francia*, § 72.

[316] Cfr. C. eur., 28.8.1991, *Brandstetter v. Austria*, § 66.

comparazione automatica tra profili del Dna, soprattutto quando le tracce a disposizione sono frutto di una commistione di profili genetici diversi, la valutazione di un esperto, successiva al confronto automatico tramite software, risulta, nella maggior parte dei casi, necessaria per stabilire un giudizio di mera compatibilità o meno fra due dati (cfr. *supra* il § 1.3)[317]. Rispetto a queste due prime categorie di dato biometrico digitalizzato, sembra che la successiva valutazione eseguita dall'operatore specializzato sia in grado, in un certo senso, di "attutire" eventuali violazioni del principio di parità tra le parti[318]. Queste sarebbero infatti poste nella condizione, pur "mediata" dall'esperto, di poter quantomeno verificare ed eventualmente falsificare il risultato di compatibilità oggetto di un controllo "manuale" eseguito da un operatore. Il fatto che un addetto specializzato in carne ed ossa sia tenuto, quantomeno per prassi[319], a verificare ed esaminare sempre il risultato (pur nella fase finale dell'attività del *tool*), costituisce «una salvaguardia di importanza fondamentale per i diritti dei singoli»[320]: l'intervento umano è, infatti, una garanzia importante, in grado di ridurre (ma non di eliminare) la probabilità che un soggetto subisca un errore valutativo da parte dell'algoritmo[321].

Non sembra possibile trarre le medesime conclusioni rispetto alla terza tipologia di dato biometrico digitale, generato automaticamente da strumenti di uso generico o commerciale, quali assistenti domestici o dispositivi elettronici di rilevamento delle proprie caratteristiche fisiologiche o comportamentali. In questo caso, l'oggetto di verifica e falsificazione delle parti non è un risultato automatico di compatibilità o meno fra due dati, successivamente ponderato e dimostrato da un operatore, ma un confronto 1:1, eseguito automaticamente dagli algoritmi di un software, il cui funzionamento potrebbe determinare, come visto, un rischio implicito per la parità delle armi. Tali informazioni non si basano su linee guida o protocolli sicuri, né sono concepiti con lo scopo specifico di essere impiegati in un procedimento. Per tale ragione, molto spesso i dati sono generati sulla base di un calcolo il cui funzionamento risulta protetto da licenze commerciali[322].

---

[317] Si concorda con A. Camon, *La prova genetica tra prassi investigative e regole processuali*, in *Proc. pen. giust.*, 2015, n. 6, p. 172, secondo il quale, con specifico riferimento alla prova genetica «ricorrere a procedure automatizzate (anziché manuali) per comparare e interpretare i profili, così da rimuovere la discrezionalità dell'operatore umano» costituisce «una soluzione prematura: molti dei programmi che eseguono questi raffronti sono "proprietari", cioè non consentono di accedere ai codici sottostanti: far fare il lavoro a quei software significherebbe quindi tagliar fuori la difesa e, più in generale, eliminare il contraddittorio intorno alla prova scientifica».

[318] Le potenziali violazioni del principio s'intendono solamente "attutite" poiché, in assenza di un'espressa regolamentazione di alcuni di questi *tools* (per es. il software S.A.R.I., v. infra il capitolo IV, § 2.1), il pericolo è quello di una complessa e confusa "battaglia fra esperti", causando una vera e propria "paralisi delle Corti". S. Quattrocolo, *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, cit. p. 122.

[319] Ci si riferisce per esempio al confronto fisionomico operato da un operatore specializzato dopo aver impiegato un software automatico di riconoscimento facciale.

[320] Cfr. J. Della Torre, *Novità dal regno unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del garante privacy d'oltremanica)*, in *www.sistemapenale.it*, 28.3.2020, p. 235.

[321] Cfr. il capitolo II, § 2.1.

[322] Su questo punto v. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, 2020, pp. 73 e ss.

Rispetto ai generali sistemi computazionali, si è già in parte accennato al fatto che la trasparenza sembra costituire l'unico e determinante "antidoto" di legittimità della trattazione automatizzata dei dati (cfr. il capitolo II, § 2.2). Il concetto di trasparenza algoritmica risulta piuttosto articolato: qualora esso sia inteso come possibilità di accedere al codice sorgente e alle operazioni eseguite dall'algoritmo, può non essere sempre utile da un punto di vista giudiziario. Tale accesso assumerebbe infatti un qualche significato, di fatto intellegibile solo all'esperto informatico coinvolto come consulente tecnico ovvero come perito. Tuttavia, come è stato rilevato in dottrina, «quando il software faccia uso di forme anche molto semplici di *machine learning*, la validazione *ex post* del risultato può diventare impossibile anche per chi lo abbia messo a punto, stante il meccanismo di autoapprendimento che lo alimenta»[323]. Per vero, la maggior parte dei software installati in *smartphone* o in dispositivi aventi un utilizzo generico o commerciale sono basati su tali tipologie di tecniche computazionali, sfuggendo, in questo modo, la possibilità per le parti di verificare o falsificare un risultato di compatibilità prodotto automaticamente dagli stessi.

In attesa di analizzare le prime pronunce giurisprudenziali in materia, i tempi sono ormai maturi per riflettere sui possibili rimedi contro gli effetti negativi scaturenti dall'opacità algoritmica[324]. A tal proposito, sarà necessario tenere in considerazione le diverse tipologie di errore di un sistema di riconoscimento biometrico, le peculiarità della modalità di comparazione 1:1 rispetto a quella 1:N,1:N+1, la fase del procedimento penale in cui sono impiegati i diversi *tool* e i diritti fondamentali, caso per caso, coinvolti. Per il momento, l'unica via per non disperdere queste informazioni potenzialmente decisive per le indagini e i procedimenti penali sembra essere quella di una sistematica verifica della metodologia certificata e applicata in conformità ad una comune "*biometric chain of custody*" (cfr. il capitolo II, § 1.3)[325].

2.2.1 Il principio del *nemo tenetur se detegere*

Da una lettura combinata degli artt. 24 co. 2 e 27 co. 2 Cost. e, a livello sovranazionale, dell'art. 6 Conv. eur. dir. uomo[326], è possibile scorgere la base normativa che garantisce all'indagato/imputato il

[323] Cfr. S. Quattrocolo, *Equo processo penale e sfide della società algoritmica*, cit., p. 141.

[324] Cfr. F. Palmiotto, *Black box on trial: the Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, cit., p. 68.

[325] Cfr. su questo punto S. Quattrocolo, C. Anglano, M. Canonico, M. Guazzone, *Technical Solutions for Legal Challenges: Equality of Arms in Criminal Proceedings*, cit., p. 17, ove si afferma che «*independent review of data generated by automated process may grant validation of evidence*».

[326] Giova specificare che la Convenzione europea non disciplina espressamente il *right to silence* ed il *priviledge against self incrimination*. Tuttavia, la Corte di Strasburgo, in diverse pronunce (cfr. C. Edu, *Funke c. Francia*, 25.2.1993, 44), ha ricondotto la tutela del principio del *nemo tenetur se detegere* entro il novero dei principi collocati nella nozione di equo processo, consacrato dall'articolo 6 Conv. eur. dir. uomo. Cfr. su questo punto T. Alesci, *Il corpo umano fonte di prova*, Wolters Kluwer, Milano, 2017, p. 24.

diritto di non collaborare con l'autorità giudiziaria[327]. Come noto, il codice di procedura penale, nell'attuazione di tale principio costituzionale, ha predisposto un sistema di norme a protezione del diritto di non collaborare attraverso divieti probatori ed inutilizzabilità speciali[328]. Invero, come già visto brevemente *supra*[329], tale garanzia si riferisce unicamente alla posizione dell'imputato, mentre l'approccio muta nei confronti delle altre parti processuali, sulle quali incombe un generale obbligo di collaborazione, in forza del principio di solidarietà sancito nell'art. 2 Cost.[330].

Con riferimento a tale garanzia, un ruolo fondamentale assume la tutela della libertà morale, dal momento che le informazioni in possesso del soggetto appartengono alla sua sfera interna e sono in grado di manifestarsi all'esterno solo grazie alla sua volontà. La libertà morale, intesa come «forma di autodeterminazione nelle proprie scelte difensive e degli atteggiamenti processuali "sul fatto proprio"»[331], trova, infatti, un diretto riscontro nella regola analoga sancita nell'art. 64, c. 2, c.p.p., a garanzia dell'imputato, ponendo la dignità della persona al centro dell'impianto codicistico. In altre parole, «quanto proviene dall'imputato, nei limiti ammessi dai diritti di libertà costituzionalmente garantiti, è utilizzabile allorché si tratti di attività volontariamente espletata (…)»; senz'altro «più delicate le implicazioni rispetto al diritto di difesa che scaturiscono allorquando l'assunzione della prova importi un minimo di attività positiva da parte dell'imputato»[332].

Nel diritto a non collaborare rientrano, pertanto, sia il diritto al silenzio sia il diritto a non compiere alcun movimento corporeo necessario alla prova nel processo penale[333]. Nel primo caso, l'imputato è «organo di prova» e il diritto si estrinseca nella facoltà di tacere di fronte all'autorità giudiziaria; nel secondo, l'imputato costituisce esso stesso l'oggetto di prova, e la garanzia consiste nella facoltà di non compiere alcun movimento fisico per consentire attività probatorie che abbiano ad oggetto il corpo[334]. Ciò detto, la sottoposizione a riconoscimento automatico dell'interessato (per es. tramite il volto), senza il suo consenso ovvero con modalità occulte, sembrerebbe stridere con tale *ratio* garantistica ove il principio in parola non solo sia interpretato nella sua dimensione dialogica con l'autorità giudiziaria, ma sia esteso anche al corpo della persona, inteso come "fonte di prova" in grado

---

[327] Cfr. M. Scaparone, *sub* art. 24 c. 2 Cost., in *Comm. Cost. Branca*, Bologna-Roma, 1981 e V. Grevi, *Alla ricerca di un processo penale "giusto". Itinerari e prospettive*, Giuffrè, Milano 2000, pp. 203 e ss. Circa la matrice storica del diritto di cui si discorre cfr. V. Grevi, *Nemo tenetur se detegere*: *interrogatorio dell'imputato e diritto al silenzio nel penale italiano***,** Giuffrè, Milano, 1972, p. 9.

[328] Cfr. T. Alesci, *Il corpo umano fonte di prova*, cit., p. 22.

[329] Cfr. il capitolo II, § 2 e il capitolo III, § 2.3.

[330] Cfr. P. Felicioni, *L'esecuzione coattiva del prelievo ematico: profili problematici*, in *Cass. pen*., 1997, pp. 316 e ss., T. Alesci, *Il corpo umano fonte di prova*, cit., p. 22 e V. Grevi, *Alla ricerca di un processo penale "giusto",* cit., p. 214 e ss.

[331] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., p. 90.

[332] Cfr. G. P. Voena, *(voce) Difesa: III) difesa penale*, in *Enc. Treccani*, Roma, 1989, p. 17.

[333] Per esempio, si pensi alla coazione esercitata per tenere un determinato comportamento per rendere più verosimile la ricognizione o per il rilascio di un saggio fonico o grafico. M. Scaparone, *Evoluzione e involuzione del diritto di difesa*, Giuffrè, Milano, 1981 e M. Scaparone, *Elementi di procedura penale, I principi costituzionali*, Giuffrè, Milano, 1999, p. 123.

[334] Cfr. F. Carnelutti, *Principi del processo penale*, Giuffrè, Milano, 1960, p. 175.

di veicolare informazioni equivalenti alle dichiarazioni di chi collabora attivamente con il proprio interlocutore[335]. Il tema concerne, pertanto, il diverso atteggiarsi del principio del *nemo tenetur se detegere* con riferimento a elementi di prova che, anche inconsapevolmente, l'imputato risulta in grado di fornire nel procedimento. A tal proposito, un esempio peculiare della *quaestio* è rappresentato dall'attività di sblocco biometrico di uno *smartphone*, ovvero di un qualsivoglia dispositivo informatico, per consentire l'accesso ai relativi contenuti da parte della polizia giudiziaria. L'osservazione dello schermo di un dispositivo elettronico posto di fronte al volto dell'indagato da parte della polizia giudiziaria può rientrare ragionevolmente tra i movimenti fisici che consentono di veicolare informazioni utili per il procedimento? Nel caso dello sblocco biometrico tramite le impronte digitali, le autorità di polizia sono legittimate ad apporre forzatamente il pollice sul lettore dello *smartphone* per accedere al suo contenuto? Per vero, cominciano a verificarsi sempre più diffusamente casi analoghi in merito ai quali le diverse Corti adite si sono cominciate a pronunciare diversamente[336]. A tal proposito, si rammenta una decisione di particolare rilievo pubblicata di recente[337], con la quale la Corte suprema olandese ha stabilito che obbligare i sospettati a fornire l'accesso biometrico al proprio *smartphone*, tramite un'impronta digitale, non costituisce una violazione del principio del *nemo tenetur se detegere*. Più nel dettaglio, in seguito al sequestro probatorio dello *smartphone*, l'indagato proprietario del dispositivo è stato ammanettato e, contro la sua volontà, è stato posizionato il suo pollice sul lettore delle impronte digitali al fine di accedere al contenuto del dispositivo. Così, vien da domandarsi ove risiede l'effettivo limite fra le attività intrusive estranee all'area protetta dalla garanzia del diritto al silenzio e gli atti che vi rientrerebbero. La Corte olandese richiama la giurisprudenza della Corte europea dei diritti dell'uomo ove, in una nota pronuncia[338], si afferma che l'acquisizione di «*material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect*» si deve ritenere compatibile con il *nemo tenetur* in quanto i mezzi intrusivi adottati avrebbero ad oggetto materiale estraneo all'area protetta dal diritto al silenzio[339]. Tuttavia, la Corte europea, in un secondo orientamento interpretativo,

---

[335] Cfr. C. Fanuele, *L'acquisizione occulta di materiale biologico*, in A.A.V.V., *Le indagini atipiche*, (a cura di) A. Scalfati, Giappichelli, Torino, 2014, p. 321.

[336] Sul punto v. https://www.lastampa.it/tecnologia/news/2019/01/16/news/la-polizia-non-puo-costringere-a-sbloccare-un-iphone-protetto-da-faceid-o-touchid-1.33671588 (visualizzato in data 6.10.2021); https://www.forbes.com/sites/thomasbrewster/2016/10/16/doj-demands-mass-fingerprint-seizure-to-open-iphones/ (visualizzato in data 6.10.2021); https://appleinsider.com/articles/16/05/02/los-angeles-court-orders-woman-to-unlock-touch-id-equipped-iphone-for-fbi (visualizzato in data 6.10.2021); https://thenextweb.com/news/fbi-uses-faceid-to-unlock-a-suspects-iphone-x-for-the-first-time (visualizzato in data 6.10.2021); https://www.fairtrials.org/news/suspects-privilege-against-self-incrimination-not-violated-when-made-unlock-smartphone (visualizzato in data 6.10.2021).

[337] Cfr. Hoge Raad, 9.2.2021, n. 19/05471, reperibile all'indirizzo https://linkeddata.overheid.nl/front/portal/document-viewer?ext-id=ECLI:NL:HR:2021:202 (visualizzato in data 6.10.2021).

[338] Cfr. *Saunders v. The United Kingdom*, 43/1994/490/672, reperibile all'indirizzo http://hudoc.echr.coe.int/webservices/content/pdf/001-58009?TID=thkbhnilzk (visualizzato in data 6.10.2021).

[339] Cfr. *Saunders v. The United Kingdom*, cit., § 69.

ha ritenuto che la garanzia in parola possa essere estesa a documenti preesistenti, come per esempio gli estratti conto del sospettato, pur presentando formalmente gli stessi requisiti oggetto del primo indirizzo ermeneutico[340]. La Corte olandese ha pretermesso questa seconda esegesi e ha ritenuto che l'impronta digitale esiste indipendentemente dalla volontà di rilasciarla da parte dell'indagato e il suo ottenimento non richiede, così, la collaborazione attiva dello stesso. Oltre a ciò, i giudici hanno dichiarato che la tecnologia di funzionamento del dispositivo oggetto di sequestro fosse al tempo così all'avanguardia che l'adozione di un metodo di accesso alternativo non sarebbe stata possibile nemmeno attraverso il ricorso ai mezzi tecnici predisposti dall'*NFI*[341]. Pertanto, la Corte olandese ha tentato di operare un bilanciamento tra la protezione dei dati archiviati nel dispositivo digitale ai fini dell'accertamento del fatto di reato, da una parte, e il rispetto della garanzia del *nemo tenetur*, dall'altra. Più nel dettaglio, richiamando la giurisprudenza della Corte di Strasburgo, secondo i giudici olandesi è necessario tenere in considerazione, oltre alle caratteristiche del materiale oggetto di indagine richiamate, anche «*the nature and degree of the compulsion, the existence of any relevant safeguards in the procedures and the use to which any material so obtained is put*»[342]. Ne conseguirebbe che, l'atto coercitivo di apporre il pollice dell'indagato sul sensore dello *smartphone*, al fine di sbloccare biometricamente il dispositivo, comportando una minima intrusione nell'integrità fisica del sospettato, non sarebbe in violazione dell'art. 6 Conv. eur. dir. uomo.

L'indirizzo interpretativo scelto dai giudici olandesi, tuttavia, non convince fino in fondo. L'evolversi costante della tecnologia impone una sistematica rivalutazione e reinterpretazione delle garanzie poste a presidio dei diritti fondamentali dell'indagato. Occorre allora cominciare a riflettere se «*the nature and the degree of the compulsion*» o, il fatto che il materiale, oggetto dell'attività coercitiva, presenti «*an existence independent*», siano da considerare, rispetto alla salvaguardia della garanzia del *nemo tenetur se detegere*, requisiti ancora idonei al contesto tecnologico attuale. Consegnare alle autorità inquirenti l'impronta digitale o addirittura il proprio volto, sebbene tale atto comporti un'impercettibile intrusione nella sfera fisica dell'indagato, addirittura pressoché nulla nel secondo caso, costituisce una forma di collaborazione che ragionevolmente può essere ricondotta alla garanzia in parola. Con riferimento al tema che rileva in questa sede, il fulcro del problema ruota attorno alla questione se, nel considerare l'attività di mettere a disposizione un proprio tratto fisico, debba prevalere l'interesse a garantire la repressione dei reati e l'individuazione dei responsabili, ovvero, il rispetto della dignità dell'uomo e di una serie di garanzie aventi rango costituzionale, altrettanto meritevoli di tutela.

[340] Cfr. *Funke v. France*, 25.2.1993, App. no. 10828/84.
[341] Cfr. *Netherlands Forensic Institute*, https://www.forensicinstitute.nl/ (visualizzato in data 7.10.2021).
[342] Cfr. *Tirado Ortiz e Lozano Martin c. Spagna* 15.6.1999, App. no. 43486/98 e *Jalloh c. Germania*, 11.7.2006, App. no. 54810/00.

Un percorso argomentativo differente s'imporrebbe, invece, nell'analisi dell'ipotesi in cui l'indagato sia destinatario della richiesta da parte della polizia giudiziaria di offrire il suono della propria voce per finalità d'individuazione ai sensi dell'art. 361 c.p.p. ovvero di ricognizione *ex* art. 213 c.p.p. Su questo punto la dottrina risulta divisa: da una parte v'è chi sostiene che l'imputato non possa essere obbligato a "parlare", escludendo necessariamente che dal rifiuto si possano dedurre elementi a carico[343], dall'altra vi sarebbe chi ritiene non invocabile un diritto alla non collaborazione con riferimento al rilascio, contro la volontà dell'indagato/imputato, di un saggio fonico[344]. Nonostante ciò, il riconoscimento vocale può avvenire ugualmente sulla base di saggi fonici posseduti dalle autorità inquirenti per altre ragioni[345]. In mancanza di questi, si è prospettata l'ipotesi di un'acquisizione "clandestina" degli stessi, senza che gli interessati ne siano direttamente informati. In questo modo, la garanzia del *nemo tenetur* non subirebbe alcuna ingerenza dal momento che essa non implicherebbe anche la facoltà dell'imputato di negare l'acquisizione al processo di qualsiasi emissione vocale a lui riconducibile. Pertanto, in questo caso, possono essere ragionevolmente acquisite registrazioni magnetofoniche offerte in un contesto extraprocedimentale, al fine di eseguire analisi tecniche potenzialmente suscettibili di produrre nei confronti dell'indagato effetti pregiudizievoli.

L'approccio più ragionevole da adottare sembra dunque essere sempre quello che considera le circostanze della fattispecie concreta oggetto di valutazione: occorre considerare le soluzioni tecnologiche che distinguono e contraddistinguono l'odierna realtà e contemperare le esigenze di rapidità dell'accertamento investigativo con la tutela della libertà di autodeterminazione dell'individuo. In un contesto giuridico che pone al centro l'inviolabilità del diritto di difesa in ogni stato e grado del procedimento, in cui l'imputato ha la garanzia di non essere considerato colpevole sino alla condanna definitiva, la libera determinazione dell'imputato se partecipare attivamente o contrastare l'azione di accertamento dei fatti oggetto di reato, fornendo o negando il proprio apporto informativo, deve continuare ad essere «un'opzione irrinunciabile»[346].

[343] Cfr. M. Biral, *L'identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, in *Rivista Italiana di Diritto e Procedura Penale*, fasc.4, 2015, p. 1842.
[344] Cfr. A. Macchia, voce *Imputato*, in *Noviss. Dig. It.*, App. IV, Torino, 1983, p. 122.
[345] A titolo esemplificativo, si pensi alla registrazione di un interrogatorio o ad un'intercettazione certamente attribuibile al soggetto.
[346] L'espressione è di V. Patanè, *Il diritto al silenzio dell'imputato*, Giappichelli, Torino, 2006, p. 80.

2.4. Il trattamento del dato biometrico digitalizzato nel rispetto del diritto alla riservatezza

Tra le garanzie individuali idonee a tratteggiare i confini di una legittima acquisizione di dati biometrici digitalizzati si ascrive anche la tutela alla riservatezza[347]. Quest'ultima, da ricondurre a livello sovranazionale agli artt. 8 Conv. eur. dir. uomo, 16 TFUE, 7 e 8 CDFUE[348], non trova invece un'espressa disciplina nella nostra Carta costituzionale e, per tale ragione, è stata collocata non sempre unanimemente[349], per via dottrinaria[350] e giurisprudenziale[351], tra i "diritti inviolabili dell'uomo" garantiti dall'art. 2 Cost.[352], conferendole un contenuto essenzialmente negativo, come pretesa di escludere altri dalla conoscenza di vicende strettamente personali e familiari.

Il termine "privacy"[353] ha radici piuttosto risalenti: quasi un secolo fa, infatti, Samuel Warren e Louis Brandeis scrivevano il celebre saggio "*The right to privacy*" in cui per la prima volta compariva l'idea del "diritto alla sfera privata che non deve essere toccata dall'Autorità pubblica" (*right to be alone*)[354]. Tale interpretazione è stata sviluppata lungo l'arco di tutto il Novecento da filosofi come

[347] Sul tema cfr. T. Alesci, *Il corpo umano fonte di prova*, cit., pp. 26 e ss., L. Luparia, *Diritto alla privacy*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*, (a cura di) L. Kalb, Giuffrè, Milano, 2019, p. 97, G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., pp. 68 e ss. e M. Torre, *Privacy e indagini penali*, Giuffrè, Milano, 2020, pp. 3 e ss.

[348] Nell'articolo 8 Conv. eur. dir. uomo è cristallizzato il diritto al rispetto della vita privata e familiare. Per un quadro aggiornato sulla giurisprudenza in materia v. COUNCIL OF EUROPE, *Guide on Article 8 of the European Convention on Human Rights*, 31.12.2020, reperibile all'indirizzo https://www.echr.coe.int/documents/guide_art_8_eng.pdf (visualizzato in data 11.10.2021). Cfr. l'art. 16 TFUE (ove si tutela il diritto di ogni persona alla protezione dei dati di carattere personale che la riguardano) e, con riferimento alla Carta dei diritti fondamentali dell'Unione europea (da qui in avanti CDFUE), cfr. l'art. 7 (diritto al rispetto della vita privata e della vita familiare) e l'art. 8 (protezione dei dati di carattere personale).

[349] Per una ricostruzione delle diverse correnti di pensiero cfr. S. Carnevale, *Autodeterminazione informativa e processo penale*, in AA.VV., *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, (a cura di) D. Negri, Aracne, Roma, 2007, pp. 9 e ss.

[350] Per una ricostruzione storica cfr. S. Rodotà, *Tecnologie e diritti*, Il Mulino, Bologna, 1995, pp. 22 e ss. Per un approfondimento sulle iniziali diverse interpretazioni dottrinarie v. S. Scagliarini, *La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio*, Aracne, Roma, 2013, pp. 43 e ss., M. Torre, *Privacy e indagini penali*, Giuffrè, Milano, 2020, pp. 7 e ss., M. Bonetti, *Riservatezza e processo penale*, Giuffrè, Milano, 2003, pp. 9 e ss., A. Barbera, *Commento all'art. 2 Cost*., in AA.VV., *Commentario alla Costituzione. Principi fondamentali*, (a cura di) G. Branca, Zanichelli, Bologna, 1975, pp. 80 e ss.

[351] Cfr. *ex multis* Cass. pen., Sez. I, 27.5.1975, n. 2129, inedita e Corte Cost., 11.6.2009, n. 173, in *Giur. Cost*., 2009, p. 4647. Sul punto cfr. anche S. Fratucello, *La protezione dei dati personali come limite all'accertamento penale*, in AA.VV., *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, (a cura di) D. Negri, Aracne, Roma, 2007, p. 120.

[352] Secondo S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica del diritto privato*, 4, 1997, p. 606, la tutela alla "privacy" andrebbe ricondotta nell'alveo dell'art. 2 Cost. e dell'art. 3 Cost. ove si menziona l'eguaglianza e la "dignità sociale". Secondo G. Di Paolo, *"Tecnologie del controllo" e prova penale*, cit., pp. 240, 241 e 242, «oltre alla clausola generale dell'art. 3 Cost. potrebbe anzitutto soccorrere l'art. 13 Cost. (…) disposizione (…) interpretata estensivamente, nel senso di ricomprendere all'interno del concetto di libertà personale anche la dignità dell'individuo», ovvero, secondo l'Autrice «si potrebbe sostenere (…) che il diritto alla riservatezza sia desumibile in via sistematica dalla tutela di una serie di diritti già esplicitamente riconosciuti dalla Carta fondamentale, e precisamente dagli artt. 13, 14, 15, 21 Cost.». Cfr. su questo punto anche S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 78.

[353] Per un primo approfondimento sulla differenza concettuale tra riservatezza e privacy cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., pp. 71 e ss.

[354] Cfr. L. D. Brandeis, S. Warren, *The Right of privacy*, in *4Harvard Law Review*, 1890, (tradotto da S. Serra), in *Ius solitudinis*, (a cura di) V. Frosini, Giuffrè, Milano, 1993. Per una ricostruzione storica cfr. M. Torre, *Privacy e indagini penali*, cit., pp. 7 e ss.

Foucault, il quale si è servito dell'evocativa e alienante struttura architettonica, ideata dal filosofo inglese Jeremy Bentham, del *Panopticon*, per rappresentare l'idea del controllo della società moderna sugli individui[355]. Giova rilevare che il diritto alla riservatezza ha presentato fin dall'inizio una mutevolezza tale da rendere difficile una precisa delimitazione dei suoi confini[356]. In seguito all'avvento delle nuove tecnologie, infatti, si è fatta sempre più strada la distinzione concettuale fra "privacy", intesa come generale «fascio di diritti»[357] riguardanti la persona, e "riservatezza" come «diritto fondamentale al controllo, da parte della stessa persona, dei dati che la riguardano»[358]. In altre parole, com'è stato osservato in dottrina, «la privacy ha smesso di essere mero "*right to be alone*", ma ha assunto una parallela "dimensione esterna", legata al controllo delle proprie informazioni»[359]. A testimonianza di questo mutamento interpretativo, la Carta dei diritti fondamentali dell'Unione europea - essendo frutto di un trasformato contesto culturale - ha conferito al singolo non solo la "tradizionale" libertà negativa di non subire interferenze nella propria sfera personale, ma anche una libertà positiva di esercitare un controllo effettivo sul flusso dei propri dati personali[360], ovvero quei contenuti informativi che permettono o agevolano l'identificazione di una persona fisica in base alle proprie caratteristiche fisiche, fisiologiche, comportamentali, allo stile di vita, alle relazioni personali, allo stato di salute, etc.[361].

Entro tale scenario, risulta certamente utile ai fini della presente ricerca approfondire, seppur per brevi cenni, come la finalità accertativa del processo penale e il diritto alla prova si possano "atteggiare" rispetto alla tutela dei dati personali. L'obiettivo di fondo allora è costituito dalla continua ricerca di un corretto bilanciamento fra l'obbligo di accertamento delle responsabilità e l'esigenza soggettiva di impedire intrusioni nella vita privata, ovvero compromissioni dell'immagine o dell'onorabilità. Su questo presupposto, infatti, il diritto alla riservatezza può subire delle limitazioni

[355] Cfr. M. Foucault, *Surveiller et punir. Naissance de la prison*, Editions Gallimard, Paris, 1975, pp. 218 e ss.
[356] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., pp. 70 e ss.
[357] Cfr. S. Rodotà, *Tecnologie e diritti*, cit., p. 107.
[358] Cfr. L. Luparia, *Diritto alla privacy*, cit., p. 102. Sul punto v. anche v. O. Pollicino, sub *Art. 8*, in AA.VV., *Carta dei diritti fondamentali dell'Unione europea*, (a cura di) R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini, Giuffrè, Milano, 2017, pp. 135 e ss.
[359] Cfr. L. Luparia, *Diritto alla privacy*, cit., p. 102.
[360] Non v'è da tralasciare il fatto che l'interpretazione giuridica di "privacy" ha assunto in alcuni sistemi di common law molti altri significati eterogenei. Infatti, sussisterebbero ben otto tipologie diverse di "privacy" (*bodily, intellectual, spatial, decisional, communicational, associational, proprietary e behavioral*), al quale potrebbe aggiungersi anche l'"*informational*". B. J. Koops, B. C. Newell, T. Timan, I. Skorvanek, T. Chokrevski, M. Galic, *A typology of privacy*, in *University of Pennsylvania Journal of International Law*, 2017, pp. 483 e ss.
[361] In questo senso cfr. M. Bassini, O. Pollicino, *Commento all'art. 8 della Carta*, in AA.VV., *Carta dei diritti fondamentali dell'Unione europea*, (a cura di) R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini, Giuffrè, Milano, 2017, p. 136.

per finalità di accertamento processuale in campo penale[362]. A tal proposito, il processo penale è stato definito, tra l'altro, come «un recettore di dati» e come «una macchina volta a cercare dati»[363]. Ad oggi, come già visto *supra* nel capitolo II[364], il sistematico impiego di dispositivi digitali ha generato, da un lato una varietà di informazioni del tutto inedita che può avere un impatto decisivo per l'andamento delle indagini e per l'accertamento dei fatti, dall'altro, ha consentito che gli stessi strumenti, a loro volta in grado di trattare e estrarre ulteriori informazioni rilevanti, costituiscano ormai un ausilio fondamentale per gli organi inquirenti per una più efficiente ricostruzione del reato. Per tale ragione, «nella dimensione tecnologica l'identità personale sembra dilatarsi, […] disperdersi, […] sino a diventare inconoscibile da parte dello stesso interessato; le informazioni riguardanti la stessa persona sono contenute in banche dati diverse, ciascuna delle quali restituisce soltanto una parte o un frammento dell'identità complessiva. Bisogna dunque fornire nuove ed idonee forme di tutela a questa identità esterna, […] frutto di un'operazione nella quale sono gli altri a giocare un ruolo decisivo, con la presenza continua di elaborazione e controllo»[365]. A tal proposito, giova sottolineare come le tecnologie di riconoscimento biometrico siano in grado di generare e trattare una grandissima quantità di dati. Impiegate per lungo tempo nel settore dei controlli alle frontiere e, con riferimento a determinati tratti biometrici, in campo investigativo, gli strumenti di riconoscimento biometrico, come visto, sono ora comunemente utilizzati anche nel settore privato (cfr. il capitolo I, § 1). Le impronte digitali, il volto, la voce o la forma dell'iride sono impiegati per prenotare pagamenti, dare accesso fisico a determinati locali di lavoro o sbloccare dispositivi mobili. Tali dati possono essere trattati e rielaborati, dunque, a fini di riconoscimento biometrico in diversi contesti[366]. In tal senso, le rappresentazioni digitalizzate dei volti e i campioni della voce costituiscono una fonte di informazioni particolarmente preziosa, in quanto consentono di riconoscere gli individui con un certo grado di probabilità sulla base delle loro caratteristiche distintive del corpo o del comportamento[367]. Pertanto, le autorità di polizia giudiziaria dispongono di diversi canali di accesso ai dati, siano da essi stessi acquisiti durante le indagini preliminari e convertiti in una rappresentazione digitale o *template*, siano

[362] Cfr. M. Bonetti, *Riservatezza e processo penale*, cit. e S. Carnevale, Autodeterminazione informativa e processo penale: le coordinate costituzionali, in AA.VV., *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, (a cura di) D. Negri, Aracne, Roma, 2007, pp. 3 e ss.

[363] Entrambe le espressioni si trovano in L. Luparia, *Diritto alla privacy*, cit., p. 104. Analogamente S. Carnevale, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in AA.VV., *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, (a cura di) D. Negri, Aracne, Roma, 2007, p. 5.

[364] Cfr. il § 1.

[365] Cfr. S. Rodotà, *Il diritto di avere diritti*, Laterza, Roma 2012, p. 319.

[366] Sono piuttosto recenti le notizie aventi ad oggetto il trattamento di dati per scopi di riconoscimento biometrico da parte di "*Facebook e Google, v. Tyron Stewart, Facebook is Using GDPR as a Means to Bring Facial Recognition Back to Europe in MobileMarketing*", reperibile su https://mobilemarketingmagazine.com/facebook-facial-recognition-eu-europe-gdpr-canada (visualizzato in data 11.10.2021) e I. Kemelmacher Shlizerman et al., *The MegaFace Benchmark: 1 Million Faces for Recognition at Scale*, (2015) reperibile su https://arxiv.org/abs/1512.00596 (visualizzato in data 11.10.2021).

[367] Cfr. il capitolo I, §§ 1 e ss.

essi provenienti da banche dati istituite da autorità pubbliche per scopi diversi da quelli di indagine e repressione dei reati (per es. per i controlli alle frontiere). Oppure, le informazioni possono provenire direttamente da privati. A tal proposito, il quadro normativo vigente è costituito dal "pacchetto protezione dati" adottato nel maggio 2016 che contempla il già menzionato regolamento (UE) 2016/679[368], "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" (cd. GDPR)[369], e la già richiamata direttiva 2016/680/UE del 27 aprile 2016[370], "relativa alla 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, nonché alla libera circolazione di tali dati" (cd. LED)[371]. Su quest'ultimo atto di diritto derivato occorre certamente soffermarsi nuovamente per stimolare alcune ulteriori riflessioni[372]. Invero, si sono già esposte *supra* le profonde perplessità circa la definizione fornita dal GDPR e ripresa dalla LED di "dato biometrico"[373]. In primo luogo, né il GDPR né la LED sembrano considerare il "formato" del dato sia nella definizione iniziale sia nelle disposizioni successive. Posto che, com'è logico, una definizione normativa debba rimanere scientificamente neutrale rispetto a questo punto[374], trattasi in realtà di un aspetto che merita maggiore attenzione da parte degli interpreti e, in particolare, dei giuristi. Nel caso infatti del *template*, la dottrina è divisa fra chi sostiene che da questo non possa in alcun modo risalirsi al soggetto a cui appartiene quel dato[375] e chi, invece, ha già dimostrato empiricamente che dai modelli elettronici biometrici si è assolutamente in grado di risalire al soggetto interessato, posto che il procedimento di digitalizzazione risulta parzialmente reversibile[376]. Ne consegue che la definizione copre qualsiasi tipologia di forma e formato del dato biometrico, purché ovviamente ne rispetti gli altri requisiti (cfr. il capitolo I, § 1). Ciò posto, al di là di alcune pregresse

[368] Cfr. il capitolo I, § 1, il capitolo II, § 2.1.
[369] Da ora in avanti GDPR.
[370] Cfr. il capitolo I, § 1.1, il capitolo II, § 2.1.
[371] Da qui in avanti LED.
[372] Cfr. il capitolo I, § 1.1. Il quadro normativo nazionale risulta costituito anche dal d.lgs. 196/2003 modificato dal d.lgs. 101/2018. Fondamentali risultano, poi, gli atti adottati dal Garante europeo, dal Gruppo di lavoro "Articolo 29" e dal Garante della *privacy* italiano.
[373] Cfr. il capitolo I, § 1.
[374] Cfr. M. Caianiello, *Conclusive remarks. Antifraud investigations and respect for fundamental rights faced with the challenge of e-evidence and digital device*, in AA.VV., *Digital Forensic Evidence. Towards Common European Standards in Antifraud Administrative and Criminal Investigation*, (a cura di) M. Caianiello, A. Camon, Wolters Kluwer, Milano, 2021, p. 243.
[375] Cfr. C. Prins, *Biometric Technology Law, Making Our Body Identify for us: Legal Implications of Biometric Technologies*, (1998) 14(3) in *Computer Law and Security Report 159*, p. 163, J. Grijpink, *Privacy Law: Biometrics and Privacy*, (2001) 17(3), in *Computer Law & Security Review 154*, pp. 156-157 e ss.
[376] Cfr. M. Bromba, *On the Reconstruction of Biometric Raw Data from Template Data*, (2006) *https://www.bromba.com/knowhow/temppriv.htm* (visualizzato in data 12.10.2021) e A. Ross, J. Shah, A. Jain, *From Template to Image: Reconstructing Fingerprints from Minutiae Points*, (2007) 29(4) in *IEEE Transactions on Patterns Analysis and Machine Intelligence*, p. 544.

considerazioni di carattere generale *supra* proposte[377], occorre soffermarsi su alcuni aspetti di particolare rilievo per il diritto alla riservatezza dell'individuo nel trattamento dei dati biometrici da parte delle autorità competenti a fini di indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. La *quaestio* di partenza può ben riassumersi nel seguente quesito: le disposizioni di diritto derivato contenute nella LED, ovvero negli atti normativi nazionali adottati dai singoli Stati membri, risultano adeguate per rispondere ai requisiti previsti dall'art. 8 della CDFUE e dall'art. 8, § 2 Conv. eur. dir. uomo?

Giova ricordare che le disposizioni poc'anzi richiamate trovano applicazione per tutte e tre le tipologie di dato biometrico digitalizzato, sia esso sotto forma di *template*, ovvero di rappresentazione digitale del campione grezzo (cd. *biometric sample*), sia esso ricavato da un video o da una fotografia digitale, ovvero derivante da dati elaborati automaticamente per uso estraneo al procedimento penale, quali assistenti domestici o dispositivi elettronici di rilevamento delle proprie caratteristiche fisiologiche e/o comportamentali. Certamente per tutte le tipologie di dato biometrico richiamate, le possibili frizioni con il diritto alla riservatezza dell'individuo potrebbero sorgere al momento dell'acquisizione e della conservazione del dato. Proprio rispetto a quest'ultima attività si tratta di verificare se il nostro sistema attuale risulti compatibile con il principio espresso più volte dalla Corte di Strasburgo secondo il quale la conservazione dei dati di carattere personale deve essere proporzionata agli scopi della raccolta e dev'essere limitata nel tempo[378]. Per vero, in diverse occasioni[379], la Corte ha stabilito che «*the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests*»[380]. Nella stessa pronuncia, la Corte prosegue affermando che «*the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences (…) fails to strike a fair balance between the competing public and private interests*»[381]. Il tema risulta di estremo rilievo anche per il sistema italiano, posto che, rispetto a determinati tratti biometrici, le disposizioni codicistiche si arrestano sulla soglia dell'elencazione dei rilievi esperibili dalla polizia giudiziaria[382].

---

[377] Cfr. il capitolo I, § 1.1.

[378] Il tema della tutela della riservatezza in presenza di attività d'indagine che potenzialmente violino il diritto alla vita privata (art. 8 Conv. eur. dir. uomo) è, infatti, stato affrontato a più riprese dalla giurisprudenza di Strasburgo.

[379] Per una completa ricostruzione v. A. Scarcella, *Conservazione delle impronte digitali degli "assolti" e violazione dell'art. 8 Conv. E.d.u.*, in *Dir. Pen. e Processo*, 2013, 7, p. 809.

[380] Cfr. *S. e Marper c. Regno Unito*, 4.12.2008 (*Requ.* nn. 30562/04 e 30566/04).

[381] Cfr. *S. e Marper c. Regno Unito*, § 125. Più di recente, nella pronuncia *Gaughran v. United Kingdom* (App. n. 45245/15), la Corte ha stabilito che «*gradation of periods of retention to reflect the seriousness of the offence involved would contribute to the goal of ensuring that the interference was no more intrusive than it required to be*».

[382] Cfr. T. Alesci, *Il corpo umano fonte di prova*, cit., p. 112.

Per esempio, nel nostro ordinamento, infatti, la conservazione delle impronte digitali o delle immagini dei volti, salve le previsioni normative generali, non è soggetta a specifici limiti temporali, rispetto ai diversi supporti che contengono il dato[383], a differenza di quanto stabilito per il Dna, in seguito all'entrata in vigore della l. 30.6.2009, n. 85[384]. Ne consegue che tale mancanza di indicazioni specifiche e a fronte di limiti temporali di conservazione anche molto dilatati, alla luce dell'introduzione del "pacchetto protezione dati" potrebbe comportare diverse problematiche di compatibilità tra la disciplina interna e quella convenzionale di cui all'art. 8, così come interpretata dalla Corte di Strasburgo.

Con riferimento alle due ulteriori categorie di dato biometrico digitalizzato[385], occorre domandarsi in quali termini il diritto alla riservatezza, architrave delle garanzie costituzionali contro le interferenze statuali, anche investigative (cfr. *supra*), mantenga il suo significato autentico di fronte alla possibilità di produrre, scambiare, conservare – ma anche carpire, intercettare, copiare – dati immateriali in uno spazio che non è più quello fisico. Peraltro, è importante tenere presente che, con riferimento alle modalità esecutive di tali attività, risulta necessario garantire il rispetto di regole idonee ad assicurare la genuinità dell'elemento acquisito nella sua "*biometric chain of custody*" (cfr. il capitolo II, § 1.2). In questo senso, giova domandarsi in che modalità le disposizioni normative contenute nel "pacchetto di protezione dei dati" si coordinino con le necessità investigative degli organi inquirenti[386].

Con riferimento alla prima delle due rimanenti categorie, le rappresentazioni video di caratteristiche biometriche possono provenire non solo da videocamere installate su richiesta di autorità giudiziarie per finalità investigative, ma anche – soprattutto – da impianti di videosorveglianza installati da soggetti privati o da soggetti pubblici[387] ovvero da videoriprese di privati cittadini[388]. Per

---

[383] Nel d.lgs. 196/2003, l'art. 57 ha demandato ad un decreto del Presidente del Consiglio dei ministri l'individuazione delle modalità di applicazione dei principi sanciti per il trattamento dei dati effettuato per le finalità di cui all'art. 53 dal Centro elaborazioni dati e da organi, uffici o comandi di polizia. E' stato introdotto il d.P.R. 15.1.2018, n. 15 recante l'articolo 10 che disciplina i termini di conservazione dei dati per ipotesi generali (cfr. *supra* il capitolo I, § 1.1).

[384] Cfr. A. Scarcella, *Conservazione delle impronte digitali degli "assolti"*, cit., p. 809. Cfr. il capitolo I, § 3.6.2. Per una ricostruzione sul livello di protezione adottato per il trattamento del Dna v. L. Scaffardi, *Giustizia genetica e tutela della persona. Uno studio comparato sull'uso (e abuso) delle Banche dati del Dna a fini giudiziar*i, Wolters Kluwer, Milano, 2017, pp. 206 e ss.

[385] Si richiamano le distinzioni già eseguite al capitolo II, § 1 e al capitolo III, § 1.

[386] Si riprende quanto già inizialmente approfondito nel capitolo I, § 1.1 e nel capitolo II, § 2.1.

[387] La normativa di riferimento che consente ai comuni di provincia di dotarsi di telecamere per finalità di pubblica sicurezza e incolumità urbana è contenuta nel d.l. 11/2009 convertito in l. 38/2009. Di recente è stato introdotto il d.l. n. 14/2017, convertito in l. 48/2017, con il quale sono stati predisposti diversi finanziamenti da parte dello Stato per l'attuazione di un sistema unitario e integrato di sicurezza per il benessere delle comunità territoriali. Inoltre, l'art. 5 *septies* del d.l. 32/2019 (cd. "sblocca cantieri"), convertito con l. 55/2019, ha stanziato un fondo di 20 milioni di euro «finalizzato all'erogazione a favore di ciascun comune delle risorse finanziarie occorrenti per l'installazione di sistemi di videosorveglianza a circuito chiuso presso ogni aula di ciascuna scuola nonché per l'acquisto delle apparecchiature finalizzate alla conservazione delle immagini».
Se gli impianti utilizzati dai Comuni sono destinati alla tutela della sicurezza urbana, le regole in materia di protezione dei dati personali sono dettate dalla direttiva 2016/680/UE (cd. LED).

[388] Per un approfondimento su questo punto, v. L. Saponaro, *L'impatto processuale delle immagini: fotografie e videoriprese*, Wolters Kluwer, Milano, 2020, pp. 67 e ss.

vero, proprio riguardo all'acquisizione di queste ultime, possono presentarsi considerazioni analoghe anche rispetto ai dati elaborati automaticamente per uso estraneo al procedimento penale. Orbene, il contesto giuridico potrebbe essere quello di una prima raccolta dei dati in conformità al GDPR, successivamente trattati e conservati seguendo le disposizioni contenute nella direttiva LED del 27 aprile 2016[389]. Più nel dettaglio, l'articolo 4 par. 2 della LED consente il trattamento dei dati personali per una qualsiasi delle finalità di cui all'articolo 1, par. 1, diversa da quella per cui sono stati previamente raccolti, nella misura in cui esso sia conforme al diritto dell'Unione o dello Stato membro e sia rispettoso dei principi di "necessità" e "proporzionalità". L'articolo 4 par. 2 della LED si applicherebbe pertanto indipendentemente dalla compatibilità con la finalità per cui i dati sono stati inizialmente raccolti. Con riferimento, però, all'interpretazione del principio di "necessità", la direttiva tace. In questo senso, il GDPR fa più volte riferimento a «una misura necessaria e proporzionata in una società democratica»[390]. Tale formulazione evoca immediatamente l'espressione contenuta nell'articolo 8 par. 2 della Conv. eur. dir. uomo, il quale stabilisce che qualsiasi ingerenza con il diritto alla vita privata e familiare deve essere prevista dalla legge e risultare necessaria in una società democratica. Rispetto, dunque, ai dati biometrici generati automaticamente da dispositivi estranei al procedimento penale, il cui impiego è stato faticosamente ricondotto *supra* all'ampia categoria delle prove atipiche, potrebbero sorgere ulteriori problematiche legate al rispetto dei principi posti a tutela del loro trattamento per l'acquisizione in giudizio. In questo senso, è stato osservato in dottrina che «*national criminal procedural law that would detail the conditions under which personal data can be requested, accessed and further used*»[391]. A tal proposito, si concorda con chi ritiene che «l'esile impalcatura dell'art. 189 c.p.p. in tema di prove atipiche non risulti idonea a soddisfare siffatte esigenze»[392]. Lo «scarno telaio dell'art. 189 c.p.p. è ben lontano dal soddisfare» l'aspettativa del singolo individuo di «mantenere il controllo» sugli «ambiti di sviluppo della [propria] vita privata», conoscendo in anticipo il «regime di comprimibilità», «poiché fissa soltanto i limiti esterni della idoneità all'accertamento dei fatti e del divieto di compromettere la libertà morale della persona, lasciando scoperti aspetti normativi essenziali del potere probatorio»[393].

In altre parole, il nostro sistema processuale, come visto *supra*, accoglie sì l'atipicità, ma entro i confini di una «"legalità probatoria", la quale, con riferimento alle misure istruttorie potenzialmente

[389] Da qui in avanti LED. Cfr. *supra* il capitolo I, § 1.1 nonché il capitolo II, § 2.1.

[390] Cfr. il considerando n. 50 e l'art. 6 par. 4 GDPR.

[391] Cfr. C. Jasserand, *Reprocessing of biometric data for law enforcement purposes*, reperibile all'indirizzo https://pure.rug.nl/ws/portalfiles/portal/90355213/Complete_thesis.pdf (visualizzato in data 15.10.2021).

[392] Cfr. C. Conti, *Sicurezza e riservatezza*, in *Dir. pen. e proc*., 2019, 11, p. 1572 e G. M. Baccari, C. Conti, *La corsa tecnologica tra costituzione, codice di rito e norme sulla privacy: uno sguardo d'insieme*, in *Dir. Pen. e Processo*, 2021, 6, p. 711.

[393] Cfr. D. Negri, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Rivista italiana di diritto e procedura penale*, Vol. 63, Nº 1, 2020, p. 26, O. Mazza, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *DPC Riv. Trim. 3/2019*, p. 12.

lesive di diritti fondamentali, non può fare a meno della tipicità»[394]. Da ciò si potrebbe dedurre che «quando non esiste una norma di rango legislativo che soddisfi – nell'*an* e nel *quomodo* – la (…) riserva [di legge], l'acquisizione non può che considerarsi vietata»[395].

Un altro esempio di mancato coordinamento fra la disciplina avente ad oggetto il trattamento dei dati biometrici e le disposizioni codicistiche sarebbe costituito altresì dalla mancata individuazione non solo dei soggetti autorizzati ad avere accesso ai dati personali raccolti per uno scopo diverso, ma anche delle specifiche categorie di individui interessati alla raccolta e acquisizione degli stessi (per es. dati biometrici di indagati, testimoni, ecc..). Peraltro, l'articolo 13 della direttiva, pur statuendo *inter alia* un diritto a richiedere al titolare del trattamento l'accesso ai dati e la rettifica o la cancellazione nonché la limitazione del trattamento dei dati personali che lo riguardano, non specifica alcun obbligo di notifica per gli interessati che li informi del trattamento, anche in una fase in cui lo scopo della raccolta risulti ormai svanito. Su questo aspetto, anche il Consiglio d'Europa sembra seguire lo stesso approccio ove ritiene che «*even if restrictions or derogations to the right to information were applied, information should be provided to the data subjects as soon as it no longer jeopardises the purpose for which the data were used*»[396].

Insomma, le disposizioni normative codicistiche e quelle derivate, contenute nel "pacchetto di protezione dei dati", non sembrano sempre rispondere adeguatamente alle esigenze di tutela alla riservatezza a fronte della possibilità di produrre, scambiare, conservare dati personali immateriali. L'impiego sempre più diffuso di dispositivi digitali che, per le loro ridotte dimensioni, possono essere trasportati ovunque, rende poi priva di significato l'applicazione della tradizionale distinzione tra luoghi pubblici e privati. Rispetto al trattamento di determinati dati biometrici digitalizzati, in specie di quelli generati automaticamente, mancherebbe un chiaro compendio delle ipotesi in cui i dati personali possono essere utilizzati (per esempio selezionando determinate categorie di reati), una descrizione trasparente delle finalità di tale impiego e un'obiettiva delimitazione del potere discrezionale esercitato dall'autorità procedente[397]. Vero che «il potere punitivo rappresenta ancora - e soprattutto oggi - il caposaldo della sovranità statuale, di fronte al quale le istanze di riservatezza di

[394] Cfr. M. Torre, *Privacy e indagini penali*, Giuffrè, Milano, 2020, p. 176.

[395] Cfr. C. Conti, *Sicurezza e riservatezza*, cit., p. 1572. L'Autrice richiama l'esempio della mancata disciplina delle videoriprese oggetto di analisi *supra* al capitolo II, § 1.4.2.

[396] Cfr. COUNCIL OF EUROPE, *The Practical Guide on the use of personal data in the police sector*, T-PD(2018)01, p. 6, reperibile all'indirizzo https://www.coe.int/en/web/data-protection/reports-studies-and-opinions#{%2220422099%22:[3]} (visualizzato in data 17.10.2021). Nello stesso senso l'interpretazione giurisprudenziale della Corte di Giustizia che, in *Tele2 Sverige e Watson e A.*, 21. 12. 2016, C-203/15 E C-698/15, § 121, afferma che «occorre che le autorità nazionali competenti alle quali è stato consentito l'accesso ai dati conservati ne diano notizia alle persone interessate, nell'ambito delle procedure nazionali applicabili, a partire dal momento in cui tale comunicazione non è suscettibile di compromettere le indagini condotte dalle autorità summenzionate. Infatti, tale informazione è, *de facto*, necessaria per consentire a dette persone di esercitare, in particolare, il diritto di ricorso (…)».

[397] Cfr. S. Quattrocolo, *Equità del processo penale e automated evidence alla luce della Convenzione Europea dei Diritti dell'Uomo*, in *Revista ítalo-española de Derecho Procesal*, Nº. 1, 2019, pp. 107-123

singoli appaiono cedevoli»[398] e «immaginare un bilanciamento interamente rimesso al legislatore è oggi illusorio»[399]. Tuttavia questo non deve legittimare a svuotare il sistema processuale della sua identità, semplificandone o escludendone le forme.

3. Alcune riflessioni conclusive

Con il presente capitolo si è inteso fornire al lettore una ricostruzione degli istituti processuali direttamente coinvolti nel trattamento del dato biometrico digitalizzato.

In conclusione al capitolo II, si è fatto cenno ai "diversi livelli di complessità"[400] che pone il dato biometrico *tout court*, considerata l'intrinseca specificità delle fonti di prova in esame: i tratti biometrici, come visto, presentano già di per sé caratteristiche ontologiche che attingono alle più differenti discipline: dalla biologia alla statistica, dalla fisica all'informatica. Ma si tratta solo del livello più basilare di complessità. Su questo si innesta infatti non solo la (successiva ed eventuale) natura digitale del dato, ma anche l'applicazione di processi automatizzati che consentono di estrarre le caratteristiche fisionomiche non direttamente visibili, rendendo agevoli confronti e valutazioni metriche. Il quadro normativo e tecnico delineato ha permesso di analizzare il trattamento del dato biometrico digitalizzato e le implicazioni scaturenti da un loro confronto automatico entro i crismi classici della nota categoria processuale della "prova scientifica", considerando, in particolare, la capacità dimostrativa di un *match* scaturente da un software di riconoscimento rispetto all'oggetto di prova e la sua intrinseca affidabilità, per poi passare alla trattazione dell'impiego dello stesso nello spettro delle garanzie fondamentali poste a tutela dell'indagato. Comprendere e risalire all'architettura e al funzionamento di questi strumenti può risultare un'operazione estremamente complessa, se non addirittura impossibile (cfr. il capitolo II, § 2.2), con evidenti potenziali ricadute su molteplici diritti fondamentali e garanzie processuali posti a presidio dell'individuo. Invero, quando questi processi automatizzati di riconoscimento sono impiegati per finalità di indagine e repressione dei reati, si potrebbero profilare delicati problemi di bilanciamento tra le esigenze di celerità ed efficienza e la tutela di alcune garanzie fondamentali. In particolare, si è inteso concentrare l'attenzione sulla finalità repressiva, tralasciando l'impiego di questi software in funzione preventiva e/o di sorveglianza da parte della polizia: la regolamentazione delle attività finalizzate a prevenire la commissione di un reato, infatti, nonostante l'attuale tendenza sia quella di una «progressiva sfumatura dei confini tra

[398] Cfr. S. Quattrocolo, *Equità del processo penale e* automated evidence, cit. p. 113.
[399] Cfr. C. Conti, *Sicurezza e riservatezza*, cit., p. 1572.
[400] Cfr. S. Quattrocolo utilizza tale espressione con riferimento ai modelli computazionali utilizzati nel campo della giustizia penale, sul punto v. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, p. 226.

prevenzione e accertamento del reato»[401], trova collocazione al di fuori del procedimento penale. Garanzie quali la libertà personale, l'equo processo e il diritto alla riservatezza sono stati solo alcuni dei parametri impiegati per valutare la legittimità dell'applicazione sistematica di software automatici di riconoscimento nei procedimenti penali, ovvero per esprimere alcune riflessioni sulle possibili condizioni di un loro potenziale utilizzo legittimo.

A questo punto della trattazione, dopo una breve ricostruzione teorica, vale la pena approfondire, nel successivo capitolo, il caso di studio dell'*automated facial recognition technology*.

[401] Cfr. S. Quattrocolo, *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Rev. Italo-espanola derecho procesal*, 2019, 1, p. 110 e F. Nicolicchia, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Diritto penale contemporaneo*, 2, 2018, p. 2.

CAPITOLO IV

AUTOMATED FACIAL RECOGNITION TECHNOLOGY E PROCEDIMENTO PENALE ITALIANO: SCENARI PRESENTI E FUTURI*

«*[T]he Court has agreed that facial recognition clearly threatens our rights. This technology is an intrusive and discriminatory mass surveillance tool. (…) We should all be able to use our public spaces without being subjected to oppressive surveillance*»[1].

(E. Bridges)

SOMMARIO: - 0. Percorso di analisi. - 1. Un'indispensabile introduzione tecnica. - 1.2. Fondamenti e limiti delle tecnologie di riconoscimento facciale. - 1.3. Le modalità di funzionamento: "in tempo reale" e "in differita". - 1.4. Finalità applicative da parte delle *law enforcement authorities*. - 1.5. Riconoscimento facciale e controlli alle frontiere. - 1.5.1. Il Sistema d'informazione Schengen. - 1.5.2. Il Sistema *European dactylographic* (EURODAC). - 1.5.3. Il Sistema di informazione visti (VIS). - 1.5.4. Il Sistema di ingressi/uscite (EES). - 2. Il volto nell'attuale impianto codicistico italiano. - 2.1. Il "Sistema Automatico Riconoscimento Immagini" e la rappresentazione digitale dei volti. - 2.1.1. Il parere del Garante nazionale sul software nelle due modalità applicative (*Real Time* vs. *Enterprise*). - 2.1.2. Il fenomeno delle "*Smart cities*": i progetti pilota di Como, Torino e Venezia. - 2.2. *Facial recognition technology* e procedimento penale in Italia. - 2.2.1. Dalle indagini preliminari… - 2.2.2. …alla corrispondenza automatica tra tipicità e atipicità probatoria. - 2.2.3. Il S.A.R.I. *Real Time*: una proposta di inquadramento. - 3. Riconoscimento facciale e diritti fondamentali coinvolti. - 3.1. L'impiego dei dispositivi in "*real time*". - 3.1.1. La libertà personale e la tutela della dignità umana. - 3.1.2. Il diritto alla riservatezza e alla protezione dei dati personali. - 3.1.3. Un noto caso di impiego del riconoscimento facciale per scopi di sicurezza e prevenzione. - 3.1.4. Libertà di espressione e manifestazione del pensiero. - 3.1.5. Libertà di riunione. - 3.1.6. Il diritto all'autodeterminazione informativa. - 3.2. L'impiego dei dispositivi in "*post remote*". - 3.2.1. Equo processo penale e parità delle armi. - 3.2.2. Il principio del *nemo tenetur se detegere*. - 3.2.3. Il trattamento del dato biometrico digitalizzato nel rispetto del diritto alla riservatezza. - 4. Il quadro normativo sovranazionale. - 4.1. *Automated facial recognition technology* e direttiva 2016/680/UE. - 4.2 Le Linee Guida del Consiglio d'Europa sull'uso del riconoscimento facciale nel settore pubblico e privato T-PD(2020)03rev4. - 4.3. Il "*Next generation Prüm*" e i possibili sviluppi del sistema di scambio e circolazione di dati. - 4.4. *Automated facial recognition technology* e la proposta di regolamento sull'intelligenza artificiale 2021/0106(COD). - 5. Considerazioni conclusive.

---

* Il presente capitolo è costituito in parte da contributi già pubblicati, v. E. Sacchetto, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2/2019, E. Sacchetto, *Biometrics as forensic evidence: some reflections from the Italian Criminal proceeding's point of view*, in *8th International Workshop on Biometrics and Forensics (IWBF)*, 2020, E. Sacchetto, *Face to face*: *il complesso rapporto tra automated facial recognition technology e processo penale*, in *www.lalegislazionepenale.it*, 16.10.2020, E. Sacchetto, *Brevi riflessioni sui fondamenti e sui limiti del rapporto fra automated faced-based human recognition technology e processo penale*, in *ASTRID*, 2022 (in via di pubblicazione), E. Sacchetto, *Automated faced-based human recognition technologies e procedimento penale alla luce della proposta di regolamento sull'IA: alcuni spunti di riflessione*, in AA.VV., *Collana del Centro Studi Giuridici del Dipartimento di Economia di Ca' Foscari*, (a cura di) C. Camardi, *atti del Convegno* **"***La via europea per l'intelligenza artificiale*", Venezia il 25-26.11.2022 (in via di pubblicazione).

[1] COURT OF APPEAL, R (Bridges) v. CCSWP e SSHD ([2020] EWCA Civ 1058).

Percorso di analisi

Con il presente capitolo, s'intende fornire al lettore un'interpretazione critica delle *automated facial recognition technologies*[2], alla luce della ricostruzione tecnico-giuridica, operata nei primi paragrafi della presente ricerca, avente ad oggetto - più in generale - il complesso rapporto fra le tecnologie di riconoscimento biometrico e il procedimento penale.

Le definizioni di base e la ricostruzione tecnica fornite nei capitoli precedenti saranno utili per comprendere e analizzare le peculiarità delle più specifiche tecniche di riconoscimento facciale, sia rispetto al tratto del volto in sé considerato, sia con riferimento al *match* scaturente da una comparazione automatizzata eseguita tramite software. Si prenderanno allora in considerazione le ormai consuete distinzioni tra i dati digitalizzati e i relativi *templates*, le rappresentazioni di tratti biometrici generati da dispositivi IoT, ovvero, immagini digitali sottoposte ad un "trattamento tecnico specifico"[3] come, per esempio, l'estrapolazione di *frames* da filmati di videosorveglianza[4]. Tale imprescindibile classificazione, rispetto alla φύσις del dato, renderà più chiare le successive e correlate proposte di classificazione nell'ambito del procedimento penale[5].

Come già anticipato brevemente *supra*[6], fra i diversi accertamenti esteriori che è possibile compiere sulla persona, il volto ha assunto negli ultimi anni un ruolo di estremo rilievo[7]. I sistemi automatizzati di riconoscimento facciale presentano il vantaggio - *inter alia* - di non richiedere alcuna collaborazione da parte del soggetto passivo: il sistema non risulta assoggettabile a cambiamenti comportamentali, volontari o meno, da parte dell'individuo sottoposto al riconoscimento (cfr. *infra* il § 1)[8]. Per tale

---

[2] Oppure *automated faced based human recognition technologies*, cfr. *ex multis* M. Jacquet, C. Champod, *Automated face recognition in forensic science: Review and perspectives*, in *Forensic Science International*, Vol. 307, 2020, pp. 1-14.

[3] Cfr. il capitolo I, § 1.

[4] Cfr. il capitolo II, § 1.

[5] Cfr. *infra* i §§ 2 e ss.

[6] Cfr. il capitolo I, § 3.3.

[7] Cfr. T. Alesci, *Il corpo umano fonte di prova*, Wolters Kluwer, Milano, 2017, p. 89, G. Gulotta, E. M. Tuosto, *Il volto nell'investigazione e nel processo. Nuova fisiognomica Forense*, Giuffrè, Milano, 2017, pp. 114 e ss., J. Zheng, V. M. Patel, R. Chellapa, *Recent developments in Video-based Face recognition*, in AA.VV., *Handbook of biometrics for forensic science*, (a cura di) M. Tistarelli, C. Champod, Springer, Cham, 2017, p. 149, N. Balossino, S. Siracusa, *L'identificazione basata sul volto: metodi fisionomici e metrici*, in https://docplayer.it/18656857-L-identificazione-basata-sul-volto-metodi-fisionomici-e-metrici.html, G. Preite, *Il riconoscimento biometrico. Sicurezza versus Privacy*, Uni Service, Trento 2007, pp. 37 e ss., F. Cascetta, M. De Luccia, *Sistemi di identificazione personale*, in *IlMonDig*, 2004, p. 49, S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, Giappichelli, Torino 2013, p. 33. V. anche il recente studio EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Person identification, human rights and ethical principles - Rethinking biometrics in the era of artificial intelligence*, December 2021, reperibile all'indirizzo https://media-exp1.licdn.com/dms/document/C4D1FAQF6LbTUaJpjVw/feedshare-document-pdf-analyzed/0/1639666588226?e=1639818000&v=beta&t=cuekRmPfKr89i09hBVr4xEM9UvjyH3CdM-Psg7WdXuo (visualizzato in data 17.12.2021).

[8] Cfr. Manfredi, E. Pessa, *Il riconoscimento dei volti: aspetti cognitivi, neuropsicologici e computazionali*, in *Sistemi Intelligenti*, fasc. 3, 2011, p. 447, A. Kumar, N. Kaur, *Face Recognition*, in *International Journal of Advanced Trends in Computer Applications (IJATCA)*, Vol. 3, no. 2, 2016, p. 10, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27.11.2019, reperibile all'indirizzo

ragione, le tecnologie di riconoscimento facciale sono state integrate in diversi dispositivi, come sistemi di telecamere a circuito chiuso o *smartphone*, rendendo sempre più agevole la verifica e la raccolta delle immagini ivi registrate. Peraltro, ad oggi, le finalità di impiego risultano le più varie[9]. Le tecnologie di riconoscimento facciale non solo possono essere sfruttate dalle forze dell'ordine per identificare e perseguire coloro che risultano sospettati di un reato[10], ma anche per ricercare persone scomparse[11], esercitare controlli alle frontiere[12], ovvero come strumento di gestione delle politiche migratorie e di rimpatrio[13]. Le tecnologie automatiche di riconoscimento facciale sono impiegate altresì all'interno degli stadi, al fine di garantire l'ordine pubblico e rendere più efficiente l'accesso alle strutture[14], durante i concerti[15], in occasione di manifestazioni pubbliche[16] e addirittura all'interno dei luoghi di culto[17]. Oltre a ciò, cominciano a diffondersi peculiari applicazioni di tali tecniche di

https://fra.europa.eu/en/publication/2019/facial-recognition (visualizzato in data 15.12.2021), R. Jafri, H. R. Arabnia, A survey of face recognition techniques, in *Journal of Information Processing Systems* 5, 2009, pp. 41–68.

[9] INFORMATION COMMISSIONER'S OPINION, *The use of live facial recognition technology in public places*, 18.6.2021, pp. 4, 17 e ss., reperibile all'indirizzo https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf (visualizzato in data 6.12.2021) e EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Person identification, human rights and ethical principles. Rethinking biometrics in the era of artificial intelligence*, 2021, pp. 14 e ss., reperibile all'indirizzo https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)697191 (visualizzato in data 30.1.2022).

[10] In questo senso *ex multis* cfr. F. Vecchio, *Le intercettazioni da remoto e i diversi modelli di bilanciamento tra esigenze investigative e diritto alla riservatezza e all'integrità dei sistemi informatici*, in *La Cittadinanza europea*, 1/2016, p. 108. Per un primo approfondimento sulle recenti politiche di sicurezza nelle città v. A.P. Paliotta, *Le politiche innovative di sicurezza nelle città tra tecnologie di riconoscimento e smart cities*, in *SINAPPSI - Connessioni tra ricerca e politiche pubbliche*, Anno X, n. 2/2020.

[11] V. a titolo esemplificativo https://findbiometrics.com/chinese-police-use-facial-recognition-find-child-abducted-30-years-ago-052107/, https://www.thehindu.com/news/cities/bangalore/face-recognition-technology-helps-find-missing-woman/article36372677.ece, https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html (visualizzati in data 6.12.2021).

[12] V. https://www.cnet.com/tech/services-and-software/us-border-patrol-used-facial-recognition-on-23-million-travelers-in-2020/, https://www.govtech.com/products/facial-recognition-to-check-pedestrians-at-border-crossing.html, https://www.biometricupdate.com/202111/paravision-expands-facial-recognition-presence-in-europe-with-new-executive (visualizzati in data 6.12.2021)

[13] Cfr. https://www.government.nl/topics/identification-documents/use-of-biometric-data-of-foreign-nationals, https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html (visualizzati in data 6.12.2021). Cfr. anche C. Dumbrava, *Artificial intelligence at EU borders: Overview of applications and key issues*, EPRS, European Parliament, 2021, reperibile all'indirizzo https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2021)690706 (visualizzato in data 17.1.2022).

[14] Cfr. S. Z. Li, A. K. Jain, *Handbook of Face Recognition*, Springer, New York, 2011, p. 373. V. anche https://www.repubblica.it/sport/calcio/2021/04/14/news/europei_sistema_sicurezza_ingresso_olimpico-296355419/ (visualizzato in data 6.12.2021).

[15] V. a titolo esemplificativo https://www.biometricupdate.com/202111/dutch-festival-promoters-split-on-face-biometrics-for-event-entry, https://www.dutchnews.nl/news/2021/10/facial-recognition-used-at-25-events-in-limburg-in-one-month-nrc/ (visualizzati in data 6.12.2021).

[16] V. https://www.fastcompany.com/90299268/brazil-is-using-facial-recognition-tech-during-rios-carnival.

[17] https://www.washingtonpost.com/news/acts-of-faith/wp/2015/07/24/skipping-church-facial-recognition-software-could-be-tracking-you/, https://evangelicalfocus.com/science/5088/brazilian-churches-start-to-introduce-facial-recognition-in-their-services. (visualizzati in data 6.12.2021).

riconoscimento anche nel settore dell'istruzione[18] e in ambito medico[19]. È ben noto il controverso caso indiano di *Aadhaar project*, finalizzato a riconoscere i cittadini mediante l'attribuzione di un cd. *Aadhaar number* - un codice unico, non riassegnabile, costituito da 12 cifre, emesso da un'apposita autorità nazionale centrale, la *Unique Identification Authority of India* (UIDAI) - per stabilire l'allocazione più efficace di sussidi, benefici, sovvenzioni e servizi pubblici ai soggetti più bisognosi e alle fasce povere della società[20]. O ancora, in Cina, entro il "sistema di credito sociale", attraverso il quale il governo assegna un punteggio (cd. *scoring*), i sistemi automatizzati di riconoscimento facciale sono impiegati per influenzare il comportamento degli individui[21] ovvero riconoscere oppositori politici, minoranze etniche e religiose[22].

Anche nel settore privato, tali tecnologie possono essere impiegate per finalità di sicurezza all'interno di esercizi commerciali, istituti bancari[23] o compagnie assicurative[24]. Tramite la registrazione e la comparazione del proprio volto è oggi possibile effettuare delle transazioni ovvero personalizzare l'offerta di acquisto per diverse categorie di clienti tramite pubblicità mirate[25]. Nell'ambito della domotica, poi, tali software automatici sono utilizzati per accedere alle proprie abitazioni, riconoscere le persone al loro interno e interagire con i dispositivi elettronici.

Proprio con riferimento alle potenzialità e alle possibili applicazioni nel settore privato dei sistemi di riconoscimento facciale, si registra un progressivo legame e una comunanza di interessi con il settore di pubblica sicurezza. In particolare, sempre più di frequente, gli organi inquirenti ovvero le autorità di pubblica sicurezza si rivolgono a intermediari privati o alle piattaforme web per

---

[18] V. https://www.ft.com/content/af08fe55-39f3-4894-9b2f-4115732395b9, https://www.telegraph.co.uk/news/2018/05/17/chinese-school-uses-facial-recognition-monitor-student-attention/. (visualizzati in data 6.12.2021).

[19] Cfr. https://eandt.theiet.org/content/articles/2019/06/facial-recognition-used-to-monitor-high-risk-hospital-patients/. (visualizzati in data 6.12.2021).

[20] Cfr. *Aadhaar Act*, n. 18/2016 reperibile all'indirizzo https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf. (visualizzato in data 6.12.2021). V. su questo F. Resta, O. Pollicino, *Riconoscimento facciale e protezione dati: attenzione al punto di non ritorno*, in *Diritti Comparati – Comparare i diritti fondamentali in Europa*, 30.1.2020.

[21] Cfr. R. Creemers, *China's Social Credit System: An Evolving Practice of Control*, in *SSRN*, 9.5.2018, pp. 1-32 e F. Liang, V. Das, N. Kostyuk, M.M. Hussain, *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, in *Policy and Internet*, 4, 10, 2018, pp. 415 e ss.

[22] Il governo cinese ricorrerebbe al *face recognition* per attività di profilazione etnico-razziale nei confronti degli Uiguri, minoranza turcofona e di fede islamica. Cfr. https://www.il-sole24ore.com/art/come-cina-usa-l-intelligenza-artificiale-controllare-uiguri-ABhvE8oB (visualizzato in data 9.11.2021).

[23] Cfr. McKinsey, *AI-powered decision making for the bank of the future*, 2021, reperibile all'indirizzo https://www.mckinsey.com/industries/financial-services/our-insights/ai-powered-decision-making-for-the-bank-of-the-future (visualizzato in data 17.1.2022).

[24] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 19 e E. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, in *Stanford Technology Law Review*, Vol. 24(1), 2021.

[25] Cfr. M. Taspinar, A. T. Naskali, G. Eren, M. Kurt, *The importance of customized advertisement delivery using 3D tracking and facial recognition*, in *2012 Second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP)*, 2012, pp. 520-524.

collezionare informazioni e dati personali rilevanti. Si pensi al dibattito suscitato dal noto caso *Clearview AI*, *start-up* di New York che ha sviluppato un sistema di riconoscimento facciale, venduto a diverse agenzie negli Stati Uniti, impiegato per riconoscere gli individui attraverso la comparazione di foto segnaletiche in possesso alle forze di polizia o di fotografie presenti negli archivi delle motorizzazioni civili e collezionando altresì le immagini pubblicate nei *social networks*[26]. Proprio con riferimento ai possibili abusi correlati all'utilizzo di questa tecnologia, alcuni Stati oltreoceano, ove diversi sistemi di sorveglianza sono particolarmente diffusi ormai da anni, stanno discutendo dell'opportunità di proibirne l'impiego alle forze di polizia e ad altre autorità pubbliche[27]. Anche alcune aziende private hanno manifestato l'intenzione di non sviluppare più tali sistemi di riconoscimento, ovvero non metterli più a disposizione delle forze di polizia[28]. Oltre a ciò, come già anticipato *supra* (cfr. il capitolo II, § 2.1) e come si avrà modo di riprendere più approfonditamente *infra* (cfr. i §§ 4 e ss.), in Europa si sta registrando una tendenza piuttosto evidente nel voler approfondire e prevenire i rischi di violazione dei diritti fondamentali derivanti dall'impiego di tali tecnologie. Già con la Risoluzione del 2019 su "*Una politica industriale europea globale in materia di robotica e intelligenza artificiale*", il Parlamento europeo aveva espresso una particolare preoccupazione per l'impiego di alcuni software di intelligenza artificiale[29], ivi compreso il riconoscimento facciale e vocale, in programmi di "sorveglianza emotiva", ossia di monitoraggio degli stati d'animo dei lavoratori e dei cittadini al fine di aumentare la produttività e conservare la stabilità sociale[30]. La Commissione europea, nel *White Paper* del 2020, aveva evidenziato alcune perplessità rispetto agli «scopi di identificazione biometrica a distanza», e per «l'impiego del riconoscimento

[26] Cfr. https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html (visualizzato in data 9.11.2021). Cfr. anche I. Neroni Rezende, *Facial recognition in police hands: Assessing the "Clearview case" from a European perspective*, in *NJECL*, 2020, vol. 11, n. 3, pp. 375 e ss., secondo la quale «*Clearview now combines its technology with a database of three billion images published on internet*», p. 376. Ne parla anche J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del Garante Privacy D'Oltremanica)*, in *www.sistempenale.it*, 28.3.2020, p. 5, Z. A. Khan, A. Rizvi, *AI based facial recognition technology and criminal justice: issues and challenges*, in *Turkish Journal of Computer and Mathematics Education*, Vol.12, No.14, 2021, pp. 3384-3392 e J. Scipione, M. Lo Monaco, *Has the horse bolted? Dealing with legal and practical challenges of facial recognition*, in *Media Laws*, 18.1.2022. Di recente il Garante per la protezione dei dati personali ha imposto una sanzione di 20 milioni di euro alla società americana *Clearview AI*, per aver posto in essere un vero e proprio monitoraggio biometrico di persone che si trovano nel territorio italiano. Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani*, 9.3.2022, comunicato stampa reperibile all'indirizzo https://www.gpdp.it/home/docweb/-/docweb-display/docweb/9751323 (visualizzato in data 9.3.2022).

[27] Cfr. J. Spivack, C. Garvie, *A Taxonomy of Legislative Approaches to Face Recognition in the United States*, in AA.VV., *Regulating Biometrics: Global Approaches and Urgent Questions*, (a cura di) A. Kak, *AI Now Institute*, 2020, pp. 89 e ss.

[28] G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 22, precisa che «la statunitense *Axon*, ovvero la più grande produttrice al mondo di videocamere indossabili (c.d. *bodycam*), ha deciso di sospendere le forniture alle forze dell'ordine, ed anche *Big Tech* come *Amazon*, *Microsoft* e *IBM* hanno annunciato una moratoria o di volere uscire dal mercato delle TRF».

[29] Da ora in avanti "IA".

[30] Cfr. PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale* (2018/2088(INI)), 12.2.2019, p. 13, reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52019IP0081 (visualizzato in data 10.11.2021).

facciale negli spazi pubblici», in quanto portatore di «specifici rischi per i diritti fondamentali»[31]. Peraltro, in una bozza preliminare del *White Paper* era stata prospettata la possibilità di proibire l'uso di queste tecnologie da parte di soggetti pubblici e privati per un periodo variabile dai tre ai cinque anni[32]. Successivamente, anche il Garante europeo per la protezione dei dati[33] e il Parlamento europeo[34] si sono allineati con questa prospettiva. Il 21 aprile 2021, poi, come visto *supra*[35], la Commissione europea ha pubblicato una proposta di regolamento «*on a European approach for Artificial Intelligence*» *(Artificial Intelligence Act)* incentrata sulla gestione e controllo dei rischi dovuti all'uso dell'IA[36]. In linea generale, i sistemi di riconoscimento biometrico impiegati "in tempo reale" e "a posteriori" sono stati classificati "ad alto rischio", poiché potenzialmente in grado di generare danni per la salute e la sicurezza o per i diritti fondamentali delle persone[37]. In particolare, l'impiego di sistemi di riconoscimento biometrico "in tempo reale" in spazi accessibili al pubblico, per finalità di contrasto, è considerato particolarmente intrusivo per i diritti e le libertà delle persone interessate[38], «nella misura in cui potrebbe avere ripercussioni sulla vita privata di un'ampia fetta della popolazione, farla sentire costantemente sotto sorveglianza e scoraggiare in maniera indiretta l'esercizio della libertà di riunione e di altri diritti fondamentali»[39]. Diversamente da quanto osservato in precedenza, nel presente capitolo si prenderà in considerazione altresì la finalità di prevenzione del reato dal momento che, negli ultimi mesi, il dibattito scientifico-giuridico intorno alla possibilità di impiegare il software nella sua modalità "*live*", per tale specifico scopo, sta raggiungendo il suo *ἀκμή*. La Commissione europea ne ha posto un generale divieto di impiego, ad eccezione di alcuni casi che, come si vedrà meglio *infra*[40], hanno sollevato diversi dubbi interpretativi. Peraltro, più di recente, il

[31] Cfr. EUROPEAN COMMISSION, *White Paper on Artificial Intelligence: a European approach to excellence and trust*, 19.2.2020, pp. 20 e ss., reperibile all'indirizzo https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_it (visualizzato in data 10.11.2021).

[32] Cfr. J. Delcker, B. Smith-Meyer, *EU considers temporary ban on facial recognition in public spaces*, in *Politico*, 16.1.2020, reperibile all'indirizzo https://www.politico.eu/article/eu-considers-temporary-ban-on-facial-recognition-in-public-spaces/ (visualizzato in data 10.11.2021).

[33] Cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust*, 29.6.2020, p. 66, reperibile all'indirizzo https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf (visualizzato in data 10.11.2021).

[34] Cfr. EUROPEAN PARLIAMENT, *Resolution "Artificial intelligence: questions of interpretation and application of international law"*, P9_TA (2021)0009, 20.1.2021, p. 56, reperibile all'indirizzo https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html (visualizzato in data 10.11.2021).

[35] Cfr. il capitolo II, § 2.1.1 e *infra* il § 4.3.

[36] Cfr. EUROPEAN COMMISSION, *Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts*, COM(2021) 206 final, reperibile all'indirizzo https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence (visualizzato in data 11.11.2021).

[37] Cfr. il capitolo II, § 3.1.

[38] Cfr. *infra* i §§ 3 e ss.

[39] Cfr. il considerando n. 18, COM(2021) 206.

[40] Cfr. il § 4.3.

Parlamento europeo con la *Risoluzione sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale*[41], ha chiesto espressamente una moratoria sulla diffusione dei sistemi di riconoscimento facciale per le attività di contrasto[42] «finché le norme tecniche non possano essere considerate pienamente conformi con i diritti fondamentali, i risultati ottenuti siano privi di distorsioni e non discriminatori, il quadro giuridico fornisca salvaguardie rigorose contro l'utilizzo improprio, un attento controllo democratico e adeguata vigilanza, e vi sia la prova empirica della necessità e proporzionalità della diffusione di tali tecnologie»[43].

Come si avrà modo di illustrare meglio nei prossimi paragrafi, non tutte le applicazioni di questa tecnologia pongono le stesse problematiche di bilanciamento fra esigenze opposte. Peraltro, come è stato opportunamente evidenziato «gli usi privati o – per così dire – "ricreativi" di queste tecnologie, (…), non devono distogliere l'attenzione dalla capacità di monitoraggio, controllo e tracciamento estremamente invasiva offerta dalle TFR, attraverso le quali è possibile ricostruire lo stile di vita, le abitudini, le preferenze, le relazioni interpersonali su larga scala»[44]. Si ritiene, dunque, che l'unica via da percorrere sia quella di «definire le condizioni necessarie per evitare che la società della sorveglianza si risolva nel controllo autoritario, nella discriminazione, in vecchie e nuove stratificazioni sociali produttive di esclusione, nel dominio pieno di una logica di mercato che cerca una ulteriore legittimazione proprio nella tecnologia»[45]. La sfida odierna è allora quella di tentare di regolare questi sistemi di riconoscimento nei loro profili più insidiosi[46], al più limitando certe applicazioni, senza porsi con un atteggiamento antistorico di chiusura e al fine di trarre il maggior beneficio in termini eticamente sostenibili in una prospettiva "*human-centred*"[47]. Certamente, il

[41] Cfr. PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale* (2020/2016(INI)), reperibile all'indirizzo https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_IT.html (visualizzato in data 11.11.2021).

[42] «(…) a meno che non siano usate strettamente ai fini dell'identificazione delle vittime di reati». Cfr. PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale*, cit., v. il § n. 27.

[43] v. il § n. 27.

[44] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 25.

[45] Cfr. S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997, p. 165.

[46] In questa direzione di recente negli Stati Uniti è stata presentata una proposta di legge federale ("*Facial Recognition Technology Warrant Act of 2019*, S. 2878", in www.congress.gov) volta a introdurre significative garanzie processuali con riguardo all'impiego da parte delle forze di polizia federali di strumenti di riconoscimento facciale. Più nel dettaglio, si prevede che le forze di polizia per attivare tali software debbano ottenere un mandato giudiziale che autorizzi l'attività. Nel corso degli anni si sono susseguite a livello statale diverse iniziative volte a limitare l'utilizzo di tali *tools* in esame, v. P. Hrick, F. Heydari, *The Growing World of Face Recognition Legislation: A Guide to Enacted and Proposed Legislation*, reperibile all'indirizzo https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5d9f7965391b2358bdccda63/1570732405589/The+Growing+World+of+Face+Recognition+Legislation.pdf (visualizzato in data 2.12.2021).

[47] Cfr. EUROPEAN COMMISSION, *Communication "Artificial Intelligence for Europe", COM(2018) 237 final*, 25.4.2018, reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN (visualizzato in data 21.1.2022), EUROPEAN COMMISSION, *Communication "Building Trust in Human-Centric Artificial Intelligence", COM(2019)*

giurista non può prendere il posto dello scienziato e viceversa. Tuttavia, si ritiene ormai necessaria l'apertura di un dialogo multidisciplinare tra giuristi ed esperti del settore che faccia emergere le principali criticità in seno al rapporto fra le diverse discipline coinvolte aventi un potenziale impatto sui diritti fondamentali. Come si illustrerà nei successivi paragrafi, i limiti derivanti dall'impiego di questi strumenti così innovativi non riguardano solo l'affidabilità della tecnologia impiegata a fini di riconoscimento, con i potenziali e correlati rischi di falsi positivi o falsi negativi[48], ma anche la concreta incapacità di reperire informazioni specifiche sulle motivazioni, modalità e conservazione dei dati così collezionati[49]. Fondamentale sarà allora, *in primis*, fornire - seguendo la linea teorica dei precedenti capitoli - una ricostruzione tecnica del funzionamento delle tecnologie di riconoscimento facciale per comprendere poi successivamente se e quali siano le lacune normative ad oggi presenti. Un valore peculiare assumeranno non solo la presentazione dei fondamenti e dei limiti delle tecniche in parola, ma anche i diversi contesti applicativi e le finalità di impiego in funzione della normativa ad oggi esistente. Infine, attraverso l'analisi empirica di S.A.R.I., "*software automatico riconoscimento immagini*", dal 2017 in dotazione alle forze di polizia italiane, si fornirà un inquadramento generale del *tool*, al fine di stabilire il corretto valore semantico da assegnare ad un risultato scaturente da un software automatico, rispetto all'accertamento dei fatti oggetto di prova.

1. Un'indispensabile introduzione tecnica

Si ritiene opportuno sin da subito rivolgere l'attenzione ai precisi meccanismi di funzionamento del procedimento entro cui si sviluppa il riconoscimento facciale, alle possibili soglie di errore, agli scopi di utilizzo e alle principali applicazioni a fini giudiziari. Nel successivo paragrafo si analizzeranno le analogie e le differenze fra tale tecnologia e la disciplina scientifica di riferimento, concentrando l'analisi sul ruolo dei processi automatizzati e dei *big data*. Questi ambiti risultano ontologicamente interconnessi e le innovazioni degli ultimi anni hanno interessato e contribuito anche al rapido sviluppo delle tecnologie di *facial recognition*.

168 final, 8.4.2019, reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0168 (visualizzato in data 21.1.2022) e EUROPEAN COMMISSION, *White Paper on Artificial Intelligence: a European approach to excellence and trust*, 19.2.2020, pp. 20 e ss., reperibile all'indirizzo https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_it (visualizzato in data 10.11.2021).

[48] Cfr. il capitolo I, § 2.5.

[49] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 21.

Come già anticipato brevemente *supra*[50], il riconoscimento facciale automatico consiste in un procedimento automatizzato di immagini digitali contenenti i volti di determinati individui[51], per finalità identificative, autenticative o di categorizzazione[52], tramite la comparazione di immagini digitali o di modelli elettronici (cd. *templates*), ossia rappresentazioni vettoriali delle caratteristiche distintive dello specifico tratto fisico considerato[53]. Da una fotografia o da un video ritraente un soggetto, è possibile ricavare l'insieme delle *features*[54], del volto generando il modello elettronico di quello specifico tratto biometrico, il quale sarà oggetto di una successiva comparazione automatizzata con un altro *template* o rappresentazione digitalizzata, precedentemente registrata. Per tale ragione, il procedimento automatico di riconoscimento costituisce un esempio di «*human-based and automated recognition of individuals based on their physical and behavioural characteristics*», ossia lo strumento che «*allows to distinguish human beings and to recognise them to a certain degree, depending on the modality, quality of the data and application*»[55]. A sua volta, pertanto, il tratto del volto - sottoposto ad un trattamento tecnico specifico - appartiene alla categoria dei "dati biometrici" così come descritta e disciplinata dagli artt. 4(14) e 9 del regolamento (UE) 2016/679 e, successivamente, ripresa da molteplici documenti normativi europei[56].

Le fasi del procedimento variano a seconda delle finalità applicative che si intendono raggiungere. Tuttavia, risulta comunque possibile, in linea generale e pur nella diversità e complessità delle più o

[50] Cfr. il capitolo I, § 3.3.

[51] Cfr. il *Parere2/2012 – WP 192 relativo al riconoscimento facciale nell'ambito dei servizi online e mobili*, 22.3.2012, reperibile all'indirizzo https://www.privacy.it/archivio/grupripareri201202.html (visualizzato in data 2.12.2021) e C. Garvie, A. Bedoya, J. Frankle, The perpetual line-up: Unregulated police face recognition in America, in *Georgetown Law, Center on Privacy & Technology*, 2016, p. 9, reperibile all'indirizzo https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf (visualizzato in data 9.12.2021).

[52] Cfr. J. Buolamwini, V. Ordóñez, J. Morgenstern, E. Learned-Miller, *Facial Recognition Technologies: A Primer*, in *Algorithmic Justice League*, 2020, pp. 2-6 e V. Manfredi, E. Pessa, *Il riconoscimento dei volti: aspetti cognitivi, neuropsicologici e computazionali*, in *Sistemi Intelligenti*, fasc. 3, 2011, p. 456.

[53] Cfr. il capitolo I, § 2.2. Per un primo approfondimento v. S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, Giappichelli, Torino, 2013, p. 33, EUROPEAN PARLIAMENT, *Regulating facial recognition in the EU*, EPRS | European Parliamentary Research Service, 2021, WORLD ECONOMIC FORUM, *A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations*, 2021, INFORMATION COMMISSIONER'S OPINION, *The use of live facial recognition technology in public places*, 18.6.2021, p. 4, reperibile all'indirizzo https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf (visualizzato in data 6.12.2021).

[54] Come già anticipato nel capitolo I, § 3.3, «i principali punti di *repere* sono: il *nasion* (radice del naso); *glabella* (punto situato al di sopra della radice del naso, dove la cute è in genere priva di peluria); *pronasale* (punto più sporgente della punta del naso); *naso spinale* (punto corrispondente al sottosetto nasale); *alare* (punto più sporgente dell'ala del naso); *prosthion* (punto superiore del solco naso labiale); *gonion* (margine inferiore del ramo della mandibola); *gnathion* (sporgenza inferiore del mento); *trichion* (punto di attacco dei capelli sulla fronte); *vertex* (punto più alto del cranio); *zygion* (punto più sporgente dello zigomo)». N. Balossino, S. Siracusa, *L'identificazione basata sul volto: metodi fisionomici e metrici*, Security Forum, Edizioni ItasForum, Bergamo, 2004, 4.

[55] Cfr. il capitolo I, § 1.

[56] Cfr. il capitolo I, § 1.

meno avanzate tecnologie di riconoscimento adottate, distinguere e semplificare, seguendo una determinata sequenza di fasi[57]. A tal proposito, il primo momento coincide con l'"acquisizione" della rappresentazione digitalizzata dell'immagine di un volto. Quest'ultima può trovarsi sotto forma di fotografia analogica, digitale ovvero *frame*, ricavata da una videoregistrazione. Tale fase può essere eseguita in un ambiente "controllato", attraverso sistemi biometrici "partecipativi", laddove si preveda la cooperazione dell'interessato durante la fase di raccolta del dato biometrico, ovvero in ambienti "non controllati", tramite sistemi biometrici "passivi" senza che l'interessato ne abbia piena consapevolezza[58]. La seconda fase è quella di "individuazione" di uno o più volti (cd. "*face detection*")[59]. Trattasi del momento in cui «si isola, all'interno dell'immagine, la presenza di un volto rispetto allo sfondo; operazione che può essere molto complessa soprattutto nei sistemi biometrici passivi»[60]. Segue, poi, la cd. "normalizzazione", ossia il procedimento di modifica e attenuazione delle variazioni del volto dovute alla posa ovvero alla scarsa o eccessiva illuminazione dell'immagine. Durante questa fase è già possibile individuare i cd. "punti di repere"[61].

In seguito, vi è il momento di "estrazione delle caratteristiche". Trattasi di uno stadio solamente "eventuale" dal momento che, come si vedrà meglio *infra*[62], le più moderne tecniche di intelligenza artificiale, durante l'apprendimento e l'analisi della rappresentazione digitalizzata del volto, permettono di ricavare le *features* tipiche, automaticamente, senza che l'estrazione delle stesse costituisca un momento a sé stante[63]. Come visto *supra* al capitolo I § 2.2, l'insieme dei tratti fondamentali del volto può essere convertito nel suo *template* o modello elettronico biometrico corrispondente, analogamente a quanto avviene per altri dati biometrici grezzi, al fine di comparare lo stesso con altri *templates* presenti all'interno di una banca dati.

A questo punto, si giunge alla fase di "registrazione" e "conservazione" della rappresentazione digitale dell'immagine, ovvero del suo modello elettronico, all'interno di un database per il successivo momento di confronto. Quest'ultimo costituisce senz'altro uno snodo fondamentale di tutto il procedimento di riconoscimento facciale, dal momento che è in tale fase che avviene la misurazione

---

[57] Cfr. S.Z. Li, A.K. Jain, *Handbook of Face Recognition*, Springer, New York, 2011, pp. 3 e ss. e C. Garvie, A. Bedoya, J. Frankle, *The perpetual line-up: Unregulated police face recognition in America*, cit., p. 9.

[58] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee-guida in materia di riconoscimenti biometrico e firma grafometrica. Allegato A al Provvedimento del Garante del 23 novembre 2014*, 12.11.2014, p. 6.

[59] V. Manfredi, E. Pessa, *Il riconoscimento dei volti: aspetti cognitivi, neuropsicologici e computazionali*, in *Sistemi Intelligenti*, fasc. 3, 2011, p. 456.

[60] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 32.

[61] Cfr. la nota n. 54.

[62] V. il successivo § 1.2.

[63] «L'estrazione delle caratteristiche può essere olistica, intesa come rappresentazione matematica dell'intera immagine facciale, come risulta dall'analisi dei suoi principali componenti; o basata sui singoli tratti biometrici, quale rappresentazione digitalizzata solamente di alcune specifiche caratteristiche localizzate del volto; o una combinazione dei due metodi (metodo di estrazione ibrido delle caratteristiche)». G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 33.

delle somiglianze tra le caratteristiche o i tratti biometrici di un modello elettronico e altri dati già registrati in un archivio di riferimento.

Rispetto alle finalità applicative di tali strumenti[64], la "verifica" o l'"autenticazione" del dato consiste nella comparazione fra due immagini con modalità 1:1. In particolare, il sistema è chiamato a verificare che l'immagine analizzata corrisponda ad un'altra conservata all'interno dello stesso *repository*[65]. Da un punto di vista biometrico-forense, invece, per "identificazione" s'intende la comparazione 1:N, 1:N+1, in cui l'immagine acquisita viene confrontata con tutte quelle presenti all'interno di una banca dati[66]. Infine, per "categorizzazione" di un'immagine, s'intende l'estrazione delle caratteristiche generali di un individuo, al fine di elaborare delle classificazioni rispetto a determinate categorie di riferimento (ad esempio, età, sesso, genere, provenienza etnica, umore, abitudini di consumo etc.)[67].

1.2. Fondamenti e limiti delle tecnologie di riconoscimento facciale

I processi automatizzati di riconoscimento facciale costituiscono un esempio paradigmatico dei "diversi livelli di complessità", la cui analisi è divenuta ormai imprescindibile per lo studio dei sistemi biometrici *tout court* impiegati a fini giudiziari (cfr. il capitolo II, § 4).

Come già sottolineato nel capitolo I, i tratti biometrici, entro i quali è possibile altresì ricondurre il volto di un individuo[68], sono caratterizzati già di per sé da meccanismi e proprietà che attingono alle più differenti discipline: dalla biologia alla statistica, dalla fisica all'informatica. Più nel dettaglio, è possibile catalogare il volto come un tratto fisico universale[69], dotato di un grado di "singolarità" dipendente dalla tecnologia utilizzata per acquisirlo e avente altresì un buon grado di invariabilità e di accettabilità[70]. Ma si tratta solo del livello più basilare di complessità. Entro tale scenario, infatti, occorre tenere in considerazione gli evidenti vantaggi offerti dall'impiego in tale settore di tecniche di intelligenza artificiale[71]. A partire dagli anni '70 del secolo scorso, la disciplina della *computer*

[64] Cfr. il capitolo I, § 2.4.

[65] Per esempio negli aeroporti, si sta diffondendo la prassi nei confronti dei passeggeri cd. "abituali" di confrontare direttamente l'immagine del volto degli stessi e la rappresentazione digitale del *chip* contenuto nel passaporto, al fine di velocizzare i controlli. FUNDAMENTAL RIGHTS AGENCY, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27.11.2019, p. 7. Un altro esempio di comparazione 1:1 è quello del riconoscimento facciale impiegato per accedere automaticamente ad un dispositivo elettronico (*smartphone*).

[66] Per esempio, tale modalità viene impiegata a fini di indagine dalla polizia giudiziaria per riconoscere un determinato soggetto.

[67] Per esempio ad alcune console di gioco sono integrati sistemi di controllo gestuale dell'utilizzatore, in grado di individuarne la fascia di età, il sesso e persino lo stato d'animo. GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobili,* 22.3.2012, p. 4.

[68] Su questo punto v. *ex multis* G. Mobilio, *Tecnologie di riconoscimento facciale,* cit., p. 11.

[69] Cfr. P. Kaur, K. Krishan, S. K. Sharma, T. Kanchan, *Facial-recognition algorithms: a literature review*, in *Medicine, Science and the Law*, 2020, vol. 60(2), p. 131.

[70] Cfr. il capitolo I, § 1.2.

[71] Cfr. il capitolo II, § 2.

vision ha compiuto un rilevante balzo in avanti, permettendo lo sviluppo di tecniche sempre più sofisticate di estrazione delle informazioni dalle immagini e dando così slancio ad uno studio specializzato nel campo del riconoscimento facciale[72]. In questo senso, le tecniche di *facial recognition* sono state ricondotte nel più esteso ambito di ricerca concernente l'IA. Oltre a ciò, tra i diversi fattori che hanno di recente decretato uno sviluppo esponenziale nella ricerca in materia vi è la disponibilità dei cd. *big data*, enormi quantità di dati o immagini raccolti in ampi database[73]. Contestualmente, il settore della *computer vision* è stato interessato da un repentino mutamento di paradigma: non è più lo sviluppatore a codificare le regole del riconoscimento, a partire dall'immagine digitalizzata di un volto, ma è il software che ricava criteri di correlazione e corrispondenza tra le immagini del *dataset* su cui è "allenato", a partire dalle *features* dei volti più ricorrenti, ossia i cd. "punti di repere"[74]. Questa transizione è stata resa possibile altresì dallo sviluppo e dall'elaborazione di algoritmi di *machine learning* in grado di riconoscere «schemi (c.d. *patterns*), o sottoschemi, all'interno di dati non strutturati, utilizzati per allenare (*training*) gli algoritmi, (…) [impiegati] allo scopo di rintracciare analoghe ricorrenze e riuscire addirittura a predire nuove correlazioni»[75]. Il *machine learning* ha poi trovato ampio sviluppo anche grazie al supporto offerto dalle cd. reti neurali artificiali[76], ossia meccanismi di elaborazione delle informazioni ispirati al funzionamento del sistema nervoso proprio delle reti neurali e del cervello umano[77]. Tali reti sono in grado di acquisire la capacità di imparare i cd. *patterns* e le associazioni esistenti fra essi, senza essere state programmate per eseguire tale operazione e apprendendo autonomamente dai propri errori[78]. Il funzionamento delle reti neurali artificiali risulta molto complesso e risalire al procedimento logico che ha portato ad uno specifico *output* di compatibilità o meno fra due volti, a partire da determinati *input*, può risultare un'attività difficilmente praticabile.

---

[72] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale,* cit., p. 38 e K.A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance,* cit., 2011, p. 31.

[73] Cfr. il capitolo II, § 2.

[74] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale,* cit., p. 52 e P. Contardo, P. Sernani, N. Falcionelli, A. F. Dragoni, *Deep learning for law enforcement: a survey about three application domains*, in *4th International Conference Recent Trends and Applications In Computer Science And Information Technology*, May 21–22, 2021, p.2.

[75] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale,* cit., p. 53.

[76] Cfr. Y. Zhu, H. Fan, K. Yuan, *Classification Mechanism of Convolutional Neural Network for Facial Expression Recognition*, in AA.VV., *Pattern Recognition. ICPR International Workshops and Challenges*, (a cura di) A. Del Bimbo, ICPR 2021, vol. 12663, Springer, Cham, pp. 1 e ss.

[77] Cfr. il capitolo II, § 2. V. sul punto G. Mobilio, *Tecnologie di riconoscimento facciale,* cit., p. 54. Sull'impiego delle reti neurali nei software di riconoscimento facciale v. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, 2020, pp. 65 e 66 e V. Manfredi, E. Pessa, *Il riconoscimento dei volti: aspetti cognitive, neuropsicologici e computazionali*, in *Sistemi intelligenti*, fasc. 3, 2011, pp. 447 e ss.

[78] Cfr. V. Manfredi, E. Pessa, *Il riconoscimento dei volti: aspetti cognitivi, neuropsicologici e computazionali*, cit., p. 456.

Infine, un ulteriore sviluppo tecnologico in questo settore si è avuto con la diffusione delle tecniche di *deep learning*[79]. In particolare, l'estrazione delle caratteristiche di *input* per ottenere i risultati di *output* può oggi avvenire in automatico per gradi di astrazione e classificazione[80]. I *patterns* presenti all'interno dei dati vengono riconosciuti a partire dai *pixel* di un'immagine digitale[81], dai rilevatori di contorni ovvero dai rilevatori della forma. Ciò ha permesso di ricavare dai dati determinate caratteristiche e proprietà anche nascoste all'interno delle immagini, consentendo non solo di determinare la presenza di un volto, ma anche di individuare analogie e differenze fra due o più individui e selezionare le immagini di volti appartenenti alla stessa persona. In questo modo, le *automated facial recognition technologies*, attraverso i calcoli probabilistici eseguiti dagli algoritmi stabiliscono la percentuale di corrispondenza tra l'immagine di un individuo e la rappresentazione digitalizzata del volto dello stesso presente in un determinato database. I risultati sono poi generalmente ordinati in base al grado di compatibilità fra le immagini comparate.

Quanto ai limiti, il volto risulta caratterizzato da un grado di "riferibilità individualizzante" più basso rispetto ad altri tratti[82]. *Features* biometriche come il Dna, le impronte digitali e l'iride, avendo ad oggetto un'informazione biologica o biochimica strutturale, permanente e ipervariabile, presentano un più alto grado di "tipicità" o "distintività"[83].

Il riconoscimento automatizzato del volto, oltre a basarsi su una caratteristica in generale poco stabile di per sé, presenta alcune difficoltà durante la fase di acquisizione del tratto. Tra gli elementi che influenzano le percentuali di falsi positivi e di falsi negativi[84], rientrano anche «la qualità e la risoluzione dell'immagine, il riflesso della luce, il movimento della persona ripresa, l'inclinazione e la posa del volto, ma anche l'età, il colore e le condizioni della pelle del soggetto, l'espressione, persino la pettinatura dei capelli o la presenza di trucco»[85]. Oltre a ciò, assume un ruolo particolare anche l'ambiente in cui l'immagine viene acquisita, entro contesti "controllati", come per esempio un ufficio di polizia o di frontiera, ovvero in ambienti entro i quali le condizioni di luce, distanza e posizionamento dell'individuo non sono controllati.

---

[79] Cfr. D. Leslie, *Understanding bias in facial recognition technologies*, in *The Alan Turing Institute*, 2020.

[80] Cfr. P. Kaur, K. Krishan, S. K. Sharma, T. Kanchan, *Facial-recognition algorithms: a literature review*, cit., p. 136.

[81] Cfr. la definizione di "*pixel*" in https://www.treccani.it/enciclopedia/pixel/ (visualizzato in data 21.1.2022).

[82] Cfr. il capitolo I, § 1.2. Sul punto v. anche K.A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*, cit., pp. 17 e ss., in cui l'Autore sostiene che «*an individual face changes considerably not only with its surface movements, but also with aging, trauma, surgery, makeup, and lighting. Faces themselves change over time, and images captured of a face can be of highly variable quality. The variability faces across populations, as well the dynamic states of the individual and the range of images that can be rendered of a particular person, make automated facial recognition a very challenging technical problem*».

[83] Cfr. il capitolo I, § 1.2 e il capitolo III, § 1.3.

[84] Cfr. il capitolo I, § 2.5.

[85] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., pp. 35-36.

Anche rispetto al più specifico settore del riconoscimento facciale automatico[86], le misure di performance di un sistema si esprimono in termini di falso positivo (o *false match rate*), in cui il software ritiene erroneamente che vi sia corrispondenza fra rappresentazioni digitalizzate o *template* di un volto[87] e di falso negativo (o *false non match rate*), in cui il *tool* stabilisce per errore una mancata corrispondenza tra le immagini[88]. Ad oggi, gli algoritmi in uso nella maggior parte dei sistemi di riconoscimento facciale risultano altamente performanti, consentendo in ambienti controllati, risultati di comparazioni 1:N, 1:N+1 con una percentuale di errore anche dello 0,1%[89]. Tuttavia, per determinare l'effettivo tasso di errore di un sistema automatico di riconoscimento facciale occorre parametrarsi rispetto a diverse variabili. In particolare, sarà necessario analizzare le caratteristiche somatiche dei soggetti destinatari dell'attività di verifica o identificazione, il preciso contesto d'impiego e le finalità del riconoscimento[90]. Proprio rispetto a queste ultime, nel paragrafo successivo si tratteranno più nel dettaglio le differenze e le analogie delle attività compiute per finalità di prevenzione e sicurezza, da un lato, e degli atti svolti a fini di indagine e repressione dei reati, dall'altro.

1.3. Le modalità di funzionamento: "in tempo reale" e "in differita"

Le modalità di funzionamento dei software automatici di riconoscimento facciale sono essenzialmente due[91]. La prima cd. "contestuale", "dal vivo" o "in tempo reale"[92], consente il riconoscimento dei volti senza ritardo o con un ritardo non significativo[93], in un'area geografica

[86] Per i sistemi di riconoscimento biometrici in generale v. il capitolo I, § 2.5.

[87] Permettendo così, per esempio, l'accesso ad un estraneo in un determinato ambiente (nella modalità "verifica", 1:1), ovvero direzionando le indagini di polizia su un soggetto sbagliato (nel caso della modalità "identificazione", 1:N, 1:N+1). Cfr. FUNDAMENTAL RIGHTS AGENCY, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27.11.2019, p. 9, reperibile all'indirizzo https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law (visualizzato in data 23.11.2021).

[88] Impedendo così, in caso di "verifica", di accedere in un determinato luogo fisico o virtuale (per esempio il sistema non permette di sbloccare lo *smartphone*), ovvero, rispetto alla modalità di "identificazione", consentendo erroneamente ad un soggetto di superare dei controlli alla frontiera. Cfr. FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27.11.2019, p. 9, reperibile all'indirizzo https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law (visualizzato in data 23.11.2021) e EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Regulating facial recognition in the EU*, 2021, p. 6, reperibile all'indirizzo https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf (visualizzato in data 6.12.2021).

[89] Cfr. P. Grother, M. Ngan, K. Hanaoka, *Face Recognition Vendor Test (FRVT). Part 2: Identification*, NIST, 2020, p. 4, reperibile all'indirizzo https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf (visualizzato in data 17.11.2021).

[90] Cfr. P. Grother, M. Ngan, K. Hanaoka, *Face Recognition Vendor Test (FRVT)*, cit., p. 8.

[91] Cfr. il capitolo I, § 1.2.

[92] O in "*real time*".

[93] Cfr. il considerando n. 8, EUROPEAN COMMISSION, *Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)*, cit., p. 21.

delimitata, attraverso flussi di video provenienti da telecamere ivi installate[94]. Tale modalità consente di monitorare specifiche aree popolate, ove sono presenti gruppi di persone numerosi e ove potrebbe sorgere un potenziale pericolo di attentati o di una minaccia per l'ordine pubblico (es. stadi, aeroporti, etc…). In questo modo, il software è in grado di collezionare le rappresentazioni digitalizzate di dati biometrici di un numero indeterminato di individui (spesso anche del tutto estranei all'attività di indagine)[95], salvo poi eseguire eventuali comparazioni con un gruppo selezionato di immagini acquisite o, in alcuni casi, conservarle per eventuali futuri *matches*[96]. Il software compara, infatti, i volti nei flussi video con quelli presenti all'interno di una banca dati predefinita e, in caso di *match* fra due rappresentazioni digitali, il sistema genera un *alert* che restituisce un risultato di compatibilità espresso in percentuale[97].

La seconda modalità è quella cd. "a posteriori"[98], in cui i dati biometrici sono già stati rilevati e il confronto e il riconoscimento avvengono solo con un ritardo significativo[99]. Trattasi di materiale, come immagini o filmati generati da telecamere a circuito chiuso o da dispositivi privati, prodotto prima che lo strumento sia impiegato nei confronti del destinatario della misura. Il sistema esegue la ricerca in automatico all'interno di una banca dati restituendo una lista di nomi simili a quello ricercato, ordinata in base ad un "punteggio" che indica il grado di similarità fra i due dati considerati. L'operatore che utilizza il software ha la possibilità di restringere la ricerca ad una porzione del database applicando dei filtri sulla base delle informazioni anagrafiche o descrittive (per es. il sesso, il colore della pelle, l'altezza, la presenza di segni caratteristici) associate alle immagini.

1.4. Finalità applicative da parte delle *law enforcement authorities*

Delle potenzialità tecnologiche dei software automatici di riconoscimento facciale poc'anzi accennate, si stanno - nel tempo - dimostrando ben consapevoli le autorità competenti in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali[100]. Tra

---

[94] Cfr. J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del Garante Privacy D'Oltremanica)*, in *www.sistemapenale.it*, 28.3.2020, p. 3.

[95] Cfr. INFORMATION COMMISSIONER'S OPINION, *The use of live facial recognition technology in public places*, 18.6.2021, p. 4, reperibile all'indirizzo https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf (visualizzato in data 6.12.2021)

[96] Cfr. E. Currao, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *DPU*, 19.5.2021, p. 5.

[97] Cfr. INFORMATION COMMISSIONER'S OPINION, *The use of live facial recognition technology in public places*, 18.6.2021, cit., p. 14.

[98] O "*post remote*".

[99] Cfr. il considerando n. 8, EUROPEAN COMMISSION, *Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)*, cit., p. 21.

[100] Sul punto v. E. Currao, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *DPU*, 19.5.2021, pp. 4 e ss., IJIS INSTITUTE, *Law enforcement Facial Recognition Use Case Catalog*, reperibile all'indirizzo https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190

le molteplici applicazioni *supra* richiamate, le tecnologie di riconoscimento biometrico si prestano in generale a forme inedite e molto pervasive di sorveglianza e *screening* di massa[101]. L'obiettivo può essere innanzitutto quello di riconoscere precocemente determinate persone da inserire in gruppi precedentemente *profiled*[102]. Se questa attività avviene in modo palese si parla di "*screening*"[103], altrimenti essa rientra tra le operazioni di "sorveglianza"[104]. Quest'ultima pratica può definirsi come la «raccolta ed elaborazione di dati personali, identificabili o meno, allo scopo di influenzare o controllare coloro ai quali essi appartengono»[105]. È intuitivo associare questa tipologia di impiego alle finalità di prevenzione di minacce alla sicurezza pubblica e agli interessi fondamentali della società tutelati dalla legge, che possono dar luogo a reati[106]. Entro certi contesti, infatti, diventa ragionevole considerare come non più sufficiente il controllo esercitato da un individuo collocato staticamente al centro di un'ipotetica area geografica di Benthamiana memoria[107]. Molteplici vicende verificatesi negli ultimi vent'anni hanno potenziato al massimo la diffusione di tecniche di analisi e rielaborazione di enormi quantità di dati e informazioni: dal caso "Echelon"[108] al cd. "controllo dei cinque occhi"[109], dalla pubblicazione di documenti riservati da parte di *WikiLeaks*[110] allo scandalo "*datagate*".

Peraltro, ad oggi non esiste nemmeno una completa panoramica sui diversi progetti pilota che coinvolgono le tecnologie di riconoscimento facciale impiegati per scopi di sicurezza, monitoraggio e prevenzione[111]. Molte aziende private del settore IT forniscono strumenti che sfruttano questa

0E786D87F74F/Law_Enforcement_Facial_Recognition_Use_Case_Catalog.pdf (visualizzato in data 23.11.2021), INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (ITIF), *The Value of Facial Recognition in Law Enforcement*, reperibile all'indirizzo https://itif.org/events/2019/07/24/value-facial-recognition-law-enforcement (visualizzato in data 23.11.2021).

[101] Cfr. F. Nicolicchia, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Wolters Kluwer, Milano, 2020, pp. 3 e ss.

[102] Il termine si riferisce ad una complessa attività di analisi denominata "*data mining*" (cfr. il capitolo II, § 1) che sfrutta la capacità dei sistemi informatici di processare una grande mole di informazioni in tempi ridotti. Su questo punto v. E. Mordini, *Il Volto e il Nome. Implicazioni Etiche, Sociali e Antropologiche delle Tecniche di Identificazione Biometriche*, in *MEDIC*, 2006, 14, p. 33.

[103] Per esempio, un controllo all'ingresso degli stadi per impedire l'accesso a soggetti daspati.

[104] A titolo esemplificativo, l'impiego di telecamere a circuito chiuso per riconoscere individui precedentemente foto-segnalati senza che i clienti di una banca sappiano che le telecamere sono dotate di sistemi di identificazione biometrica.

[105] Cfr. D. Lyon, *La società sorvegliata*. *Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2002, p. 2.

[106] Per la disciplina del trattamento dei dati con finalità di prevenzione di minacce alla sicurezza pubblica a e agli interessi fondamentali della società tutelati dalla legge che possono dar luogo a reati v. la Direttiva 2016/680/UE. Cfr. il capitolo I, § 1.1.

[107] Cfr. J. Bentham, *Panopticon ovvero la casa d'ispezione*, Marsilio, Venezia, 1983, 1997, pp. 37 e ss.

[108] "Echelon" è il programma di sorveglianza condotto tramite intercettazioni di telecomunicazioni che è stato praticato, anche in Europa, su accordo di USA, Canada, Australia, Nuova Zelanda, Regno Unito (c.d. *Five Eyes*), tra la fine degli anni '90 e l'inizio degli anni 2000. Ne parla anche G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 14.

[109] V. nota precedente.

[110] Sito web fondato da Julian Assange al fine di pubblicare documenti riservati coperti dal segreto di Stato ovvero di aziende messi a disposizione in forma anonima in seguito a fughe di notizie (cd. *leaks*) non rintracciabili. V. su questo tema G. Ziccardi, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, Milano, 2015, pp. 166 e ss.

[111] Cfr. FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., p. 11. A titolo esemplificativo v. E. Mureddu, *Come Venezia è diventata il grande fratello d'Europa*, 27.10.2021, reperibile all'indirizzo https://europa.today.it/attualita/venezia-grande-fratello.html (visualizzato in data 2.12.2021).

tipologia di riconoscimento servendosi così di modalità di controllo e sorveglianza sempre più sofisticate[112]. Tale capacità di tracciamento sta diventando sempre più pervasiva e rispondente alle più disparate finalità[113]. In ambito pubblico, l'impiego di questi *tools* si presta alle attività volte a riconoscere e perseguire gli individui sospettati di un reato, ricercare persone scomparse[114] o ancora, come si avrà modo di approfondire *infra*, al fine di esercitare controlli alle frontiere e come strumento di gestione delle politiche migratorie e di rimpatrio[115].

Risulta pertanto ragionevole associare e catalogare rispettivamente le due modalità di funzionamento dei sistemi di riconoscimento facciale poc'anzi descritte al raggiungimento di alcune determinate finalità. In altre parole, l'impiego del software in via "contestuale", "dal vivo" o "in tempo reale" si presta più ad un impiego per finalità di prevenzione della commissione di una fattispecie di reato, potendo rientrare tra le pratiche di *policing*[116]. Tale area, connessa all'ambito dell'*intelligence*, si colloca al di fuori del procedimento penale e sfugge, come noto, ad una regolamentazione rigida e precisa. Del resto, com'è stato rilevato in dottrina « (…) *constraining it with strict boundaries would condemn it to be less effective*…»[117]. L'assenza di un chiaro quadro giuridico di riferimento in questo settore rende più complesso tratteggiare efficacemente i contorni della materia. Come si approfondirà meglio *infra*, infatti, il rischio è quello di legittimare pericolosi squilibri tra poteri autoritativi ed esigenze securitarie, da un lato, e libertà fondamentali, dall'altro. Per usare le parole della Corte europea dei diritti dell'Uomo, l'effettivo pericolo è quello di «*undermine or even destroy democracy under the cloak of defending it*»[118]. Inoltre, come è stato anticipato *supra*[119], il *tool* di riconoscimento facciale impiegato in tempo reale potrebbe essere pensato anche come "mezzo di ricerca della prova", finalizzato alla ricerca e all'acquisizione di elementi o tracce, da cui poter trarre informazioni utili per l'accertamento dei fatti.

La modalità "a posteriori", invece, rende lo strumento compatibile con il raggiungimento delle finalità di indagine e repressione dei reati. Anche rispetto a risultati di compatibilità scaturenti

---

[112] Cfr. D. Lyon, *La società sorvegliata*, cit., pp. 2 e ss. e S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, (trad. it.) P. Bassotti, Luiss, Roma, 2019, pp. 19 e ss.

[113] I dati generati automaticamente tramite dispositivi IoT, per esempio, divengono una preziosa fonte di scambio tra i cd. *Big Tech*. V. Su questo G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 15.

[114] Cfr. J. Shuppe, *How Facial Recognition Became a Routine Policing Tool in America*, in *NBC NEWS*, 11 maggio 2019, reperibile all'indirizzo https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251 (visualizzato in data 1.12.2021).

[115] Cfr. D. Harwell, *FBI, ICE Find State Driver's License Photos are a Gold Mine for Facial-Recognition Searches*, in *The Washington Post*, 7.7.2019, reperibile all'indirizzo https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/ (visualizzato in data 1.12.2021).

[116] Sulla distinzione fra "*policing*" o "*prevention*" e "*repression*" v. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, pp. 22 e 38.

[117] Cfr. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, cit., p. 22.

[118] Cfr. C. Edu, *Big brother watch c. Regno Unito*, 13.9.2018, 308.

[119] Cfr. il capitolo II, § 1.4.2.

automaticamente da dispositivi di uso commerciale si potrebbero ragionevolmente desumere utili elementi di prova[120].

1.5. Riconoscimento facciale e controlli alle frontiere

1.5.1. Il Sistema d'informazione Schengen

Vale la pena di fare cenno, a questo punto della trattazione, alla disciplina riguardante i principali sistemi di scambio di dati e informazioni all'interno dell'Unione europea per finalità di gestione dell'immigrazione e contrasto al crimine e al terrorismo. Infatti, negli ultimi vent'anni si è assistito ad un ricorso sempre più frequente da parte delle istituzioni europee e degli Stati membri a strumenti tecnologici di sorveglianza basati sul trattamento di dati biometrici[121]. Trattasi di una vera e propria "digitalizzazione della politica europea e di immigrazione"[122], che tende verso una sempre maggiore integrazione e interoperabilità fra le diverse banche dati[123]. Come è stato anche evidenziato in dottrina, l'obiettivo è quello di «confrontare le immagini facciali catturate dalle forze dell'ordine […] con i dati contenuti nei diversi database a livello europeo, ampliando a dismisura le potenzialità di controllo cui ciascuno di essi è preposto, ad esempio, in ambito migratorio nel rilascio dei visti, nelle richieste di asilo, e persino nella più generale tutela della sicurezza pubblica»[124].

Soprattutto in seguito agli atti terroristici dell'11 settembre 2001 ed agli attentati di Madrid e Londra del 2004 e 2005, il "Sistema d'informazione Schengen", da strumento concepito inizialmente per il controllo delle frontiere, è divenuto un efficiente *tool* di indagine e tutela della sicurezza interna degli Stati[125]. In particolare, con l'introduzione del "Sistema d'informazione Schengen di seconda

---

[120] Cfr. il capitolo II, § 1.

[121] Cfr. N. Vavoula, *Databases for Non-EU Nationals and the Right to Private Life: Towards a System of Generalised Surveillance of Movement?*, in AA.VV., *EU Law in Populist Times*, (a cura di) F. Bignami, Cambridge University Press, Cambridge, 2020, pp. 227 e ss., L. Carrer, R. Coluccini, *Tecnologie per il controllo delle frontiere in Italia identificazione, riconoscimento facciale e finanziamenti europei*, in *Hermes Center for Transparency and Digital Human Rights*, 2021, pp. 7 e ss., reperibile all'indirizzo https://www.documentcloud.org/documents/21128523-tecnologie-per-il-controllo-delle-frontiere-in-italia-identificazione-riconoscimento-facciale-e-finanziamenti-europei (visualizzato in data 6.12.2021) e EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Artificial intelligence at EU borders, Overview of applications and key issues*, IDA, 2021, pp. 13-14, reperibile all'indirizzo https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf (visualizzato in data 18.1.2022).

[122] Cfr. M. Besters, F.W.A. Brom, *"Greedy" Information Technology: The Digitalization of the European Migration Policy*, in *European Journal of Migration & Law*, 12, 4, 2010, pp. 462 e ss.

[123] Su quest'ultimo aspetto, cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., pp. 269 – 285 e Comunicazione della Commissione al Parlamento europeo e al Consiglio, "*Strategia per uno spazio Schengen senza controlli alle frontiere interne pienamente funzionante e resiliente*", COM(2021) 277 final del 2.6.2021.

[124] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 250.

[125] Il SIS è caratterizzato da una struttura complessa finalizzato ad eseguire attività di controllo alle frontiere, controllo doganale, contrasto ai reati di terrorismo, altri gravi reati o esecuzione di sanzioni penali, decisioni in materia di ingresso e soggiorno di cittadini di Paesi terzi e controlli di sicurezza sui cittadini di Paesi terzi che fanno richiesta di protezione internazionale. Il SIS si articola poi in una rete di SIS nazionali (N-SIS), situati presso ciascuno Stato membro e dotati di un'interfaccia nazionale uniforme (NI-SIS) e di un database centrale (C-SIS), collocato a Strasburgo. Il sistema consente lo scambio dei dati in una rete virtuale

generazione" (cd. SIS II) sono state ampliate le funzionalità dello strumento e si è prevista la possibilità di collezionare e registrare dati biometrici, quali le impronte digitali e le immagini dei volti. In seguito alla riforma del "Codice delle frontiere Schengen" del 2016[126] il SIS II è stato ulteriormente modificato e implementato e ad oggi la disciplina di riferimento è contenuta in tre regolamenti distinti che a breve entreranno in vigore[127].

Con riferimento ai dati trattati, è interessante sottolineare che il sistema può archiviare o lanciare ricerche utilizzando come dato la rappresentazione digitalizzata del volto, al fine di segnalare persone ricercate (SIS-polizia)[128], respingere o rifiutare il soggiorno, ovvero ordinare provvedimenti restrittivi (SIS-frontiere)[129] o, ancora, disporre il rimpatrio (SIS-rimpatri)[130]. Più nel dettaglio, tali immagini possono essere impiegate solamente per confermare l'identità di un soggetto già individuato grazie ad una precedente interrogazione tramite dati alfanumerici[131]. Viene inoltre specificato che l'inserimento e il trattamento delle immagini dei volti nel SIS «dovrebbe essere limitato a quanto necessario ai fini degli obiettivi perseguiti, dovrebbe essere autorizzato dal diritto dell'Unione, dovrebbe avvenire nel rispetto dei diritti fondamentali, in particolare dell'interesse superiore del minore, e dovrebbe essere conforme alla normativa dell'Unione in materia di protezione dei dati»[132]. Peraltro, si aggiunge che «non appena ciò diviene tecnicamente possibile, e garantendo al contempo un grado elevato di affidabilità dell'identificazione, è possibile ricorrere a fotografie e immagini del volto per identificare una persona presso valichi di frontiera regolari»[133]. Sembra dunque che i processi automatizzati di riconoscimento facciale siano destinati a divenire uno degli strumenti principali al fine di raggiungere i succitati obiettivi. Per vero, il Garante europeo in più occasioni ha espresso le sue preoccupazioni in

cifrata tra gli uffici della SIRENE (*Supplementary Information Request at the National Entries*), strumento ausiliario del SIS, i cui uffici sono collocati a livello nazionale per fornire informazioni supplementari rispetto alle segnalazioni ricevute. Per un approfondimento v. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., pp. 253 e ss.

[126] Cfr. il regolamento (UE) 2016/399, reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/it/LSU/?uri=CELEX%3A32016R0399.

[127] Cfr. il regolamento (UE) 2018/1862 del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione, regolamento (UE) 2018/1861 del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006 e il regolamento (UE) 2018/1860 del 28 novembre 2018, relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare.

[128] Cfr. Artt. 26, 32, 34, 36, 38 e 40 del regolamento (UE) 2018/1861.

[129] Cfr. Artt. 24 e 25 del regolamento (UE) 2018/1861.

[130] Cfr. Art. 4, par. 1, lett. *u*) del regolamento (UE) 2018/1860.

[131] Cfr. Art. 43, par. 1, regolamento (UE) 2018/1862 e art. 33, par. 1, regolamento (UE) 2018/1861.

[132] Cfr. il considerando n. 20 dei regolamenti (UE) 2018/1862 e 2018/1861.

[133] Cfr. l'art. 43, par. 4 del regolamento (UE) 2018/1862 e art. 33, par. 4 del regolamento (UE) 2018/1861.

merito allo standard di qualità dei dati utilizzati, alla necessità e alla proporzionalità dell'impiego dei volti come indicatore biometrico preposto al raggiungimento degli scopi indicati[134].

1.5.2. Il Sistema *European dactylographic* (EURODAC)

Come noto, il regolamento n. 2725/2000/CE ha istituito l'EURODAC, ossia il database europeo delle impronte digitali di coloro che fanno richiesta di asilo e delle persone che attraversano la frontiera irregolarmente. La *ratio* dell'istituzione di tale banca dati sarebbe quella di agevolare l'individuazione dello Stato responsabile per la valutazione delle domande di protezione internazionale proposte da cittadini di Paesi terzi o da apolidi. Il sistema, infatti, permette di comparare le impronte digitali dei richiedenti asilo, ovvero degli immigrati irregolari nell'area di Schengen, che abbiano fatto più volte richiesta in Stati diversi (cd. *asylum shopping*).

Grazie al regolamento (UE) 603/2013, poi, le autorità di contrasto possono accedere ai dati biometrici raccolti, garantendo alcuni diritti minimi dei soggetti sottoposti al rilevamento degli stessi[135]. La raccolta e l'accesso a EURODAC, tuttavia, deve essere ritenuto «necessario in un caso specifico (vale a dire non si eseguono confronti sistematici)», e si deve procedere «a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri gravi reati», nel caso in cui sussistano «fondati motivi per ritenere che il confronto contribuisca in misura sostanziale alla prevenzione, all'individuazione o all'investigazione di uno dei reati in questione»[136].

Nel 2016, nell'ambito di una serie di riforme del "sistema Dublino"[137], si è tra l'altro proposto di estendere alle immagini dei volti la categoria dei dati da raccogliere, archiviare e trasmettere alle autorità di sicurezza pubblica[138]. Peraltro, proprio con riferimento a quest'ultimo aspetto, il Garante europeo aveva già in precedenza sollevato alcuni dubbi circa il rispetto dei principi di proporzionalità

---

[134] Cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 7/2017, on the new legal basis of the Schengen Information System, 2.5.2017*, p. 6, reperibile all'indirizzo https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_en.pdfm (visualizzato in data 6.12.2021).

[135] Cfr. l'art. 29 del regolamento (UE) 603/2013.

[136] Cfr. l'art. 20, par. 2 del regolamento (UE) 603/2013.

[137] Su questo v. P. De Pasquale, *Verso la rifusione del regolamento "Dublino III"*, in *Studi sull'integrazione europea*, 2018, 2, pp. 267 e ss.

[138] Cfr. l'art. 2 della proposta di riforma del regolamento nella sua ipotetica nuova formulazione, reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0272(01)&from=nl (visualizzato in data 7.12.2021), ove specifica che « (…) *taking fingerprints and facial images of minors from the age of six shall be carried out in a child-friendly and child-sensitive manner by officials trained specifically to enrol minor's fingerprints and facial images. The minor shall be informed in an age-appropriate manner using leaflets and/or infographics and/or demonstrations specifically designed to explain the fingerprinting and facial image procedure to minors and they shall be accompanied by a responsible adult, guardian or representative at the time their fingerprints and facial image are taken. At all times Member States must respect the dignity and physical integrity of the minor during the fingerprinting procedure and when capturing a facial image*».

e di necessità nel trattamento di questi dati[139]. La raccolta sistematica di dati biometrici eseguita nei confronti di soggetti oggettivamente posti in una condizione di particolare vulnerabilità e di marginalizzazione crea già di per sé evidenti disparità di trattamento rispetto a tutti gli altri cittadini europei. Estendere tale pratica anche alle immagini dei volti solleverebbe diversi dubbi circa «*the need to collect and use the facial images of the categories of persons addressed in the Eurodac recast Proposal and of the proportionality of their collection, relying on a consistent study or evidence-based approach*»[140].

1.5.3. Il Sistema di informazione visti (VIS)

Ulteriore strumento sul quale vale la pena soffermarsi brevemente è il "Sistema di informazione visti" (VIS), posto a presidio dei controlli alle frontiere dello spazio Schengen e finalizzato allo scambio di dati e informazioni sui visti rilasciati dai Paesi membri ai cittadini di Paesi terzi[141].

Il VIS si compone di un "*Central Visa information system*" (CS-VIS) avente sede a Strasburgo con il quale si interfacciano le diverse sezioni nazionali ("*The National Interfaces*"). Esso persegue la duplice finalità di costruire una politica comune in materia di visti e rafforzare le politiche di sicurezza pubblica, operando controlli sempre più diffusi alle frontiere e all'interno degli Stati membri, disponendo di strumenti di riconoscimento sempre più efficienti e mettendo in atto una politica di prevenzione di minacce alla sicurezza interna sempre più serrata[142].

Oltre al trattamento dei dati alfanumerici, come le generalità, la provenienza e lo scopo del viaggio, è prevista la raccolta delle impronte digitali e delle fotografie. Queste ultime sono utilizzate solo come strumento secondario di verifica dell'identità, qualora l'operazione di identificazione non vada a buon fine con altri elementi. Invero, di recente, in seguito agli attentati terroristici del novembre 2015 e del marzo 2016, sono state introdotte nuove disposizioni per implementare VIS tramite l'impiego delle tecnologie di riconoscimento facciale[143]. Lo scopo è quello di collezionare altresì le immagini dei volti

---

[139] Cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation*, 5.9.2012, reperibile all'indirizzo https://edps.europa.eu/sites/edp/files/publication/12-09-05_eurodac_en.pdf (visualizzato in data 7.12.2021).

[140] Cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 07/2016 on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)*, 21.9.2016, p. 9, reperibile all'indirizzo https://edps.europa.eu/sites/edp/files/publication/16-09-21_ceas_opinion_en.pdf (visualizzato in data 7.12.2021).

[141] V. il regolamento (CE) 767/2008 e la Decisione 2008/633/GAI. Per un approfondimento v. M. Gialuz, *Principio di accessibilità e banche dati di "primo pilastro"*, in AA.VV., *Cooperazione informativa e giustizia penale nell'Unione europea*, (a cura di) F. Peroni, M. Gialuz, EUT - Edizioni Università di Trieste, Trieste, 2009, pp. 139-163.

[142] Cfr. l'art. 5, par. 1, lett. *b*) e *c*) del regolamento (CE) 767/2008.

[143] Cfr. regolamento (UE) 2021/1134 del Parlamento europeo e del Consiglio del 7 luglio 2021 che modifica i Regolamenti (CE) n. 767/2008, (CE) n. 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 e (EU) 2019/1896 del Parlamento europeo e del Consiglio e che abroga le Decisioni 2004/512/CE e 2008/633/GAI del

già digitalizzate[144], al fine di poterle impiegare per successive comparazioni in sistemi automatizzati di confronto[145]. Questa raccolta dati è stata estesa anche ai soggetti minorenni e ai titolari di visti per soggiorno di lunga durata e di permessi di soggiorno. Ciascun dato personale che figura nella domanda dovrebbe essere confrontato con i dati registrati nei seguenti sistemi di informazione e banche dati: «il VIS, il SIS, il sistema di ingressi/uscite (EES), il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), Eurodac, il sistema europeo di informazione sui casellari giudiziari per i cittadini di paesi terzi (ECRIS-TCN) limitatamente a condanne per reati di terrorismo o altre forme di reati gravi, i dati Europol, la banca dati Interpol sui documenti di viaggio rubati e smarriti (SLTD), la banca dati Interpol sui documenti di viaggio associati a segnalazioni (TDAWN), l'elenco di controllo ETIAS di cui al regolamento (UE) 2018/1240 del Parlamento europeo e del Consiglio»[146].

1.5.4. Il Sistema di ingressi/uscite (EES)

Infine, il "Sistema di ingressi/uscite" (*Entry/exit System* – EES)[147], disciplinato dal regolamento (UE) 2017/2226 del 30.11.2017, è finalizzato sia al controllo dei cittadini di Paesi extra-UE che transitano nello spazio Schengen per periodi di breve durata, sia all'esecuzione di operazioni di *law enforcement*, quali il supporto alla lotta al terrorismo e ai crimini gravi.

La struttura organizzativa del sistema è analoga a quelle di altri strumenti descritti in precedenza (v. *supra*); è prevista la creazione di un fascicolo individuale in cui sono conservati i dati sull'identità, i documenti di viaggio e i dati biometrici. Tra questi ultimi, si ricomprende l'immagine del volto, definita espressamente come "dato biometrico"[148], specificando altresì che l'immagine, «rilevata sul posto» ovvero «estratta in formato elettronico dal chip degli eMRTD (*Machine Readable Travel Document* – documenti di viaggio elettronici a lettura ottica)», debba presentare le «specifiche in termini di qualità e risoluzione stabilite per l'inserimento nell'EES»[149], al fine di poterla impiegare «nel confronto biometrico automatizzato»[150].

Consiglio, ai fini della riforma del sistema di informazione visti, reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32021R1134 (visualizzato in data 7.12.2021).

[144] Cfr. il capitolo I, § 2.2.

[145] V. il considerando n. 12 del regolamento (UE) 2021/1134.

[146] Cfr. il considerando n. 15 del regolamento (UE) 2021/1134.

[147] Da qui in avanti EES.

[148] Cfr. l'art. 3, par. 1, nn. 17 e 18 del regolamento (UE) 2017/2226.

[149] Cfr. l'art. 15, parr. 2 e 4 del regolamento (UE) 2017/2226.

[150] Cfr. l'art. 15, par. 4 del regolamento (UE) 2017/2226.

Con il "Sistema europeo di informazione e autorizzazione ai viaggi" (ETIAS)[151], l'EES realizza un insieme di attività di raccolta e registrazione di dati biometrici rivolte ai viaggiatori all'interno dell'area Schengen. Proprio con riferimento a ciò, ci si domanda se questa collezione sistematica di dati possa dirsi rispettosa del principio di proporzionalità, sancito dall'art. 52 par. 1 della Carta dei diritti fondamentali dell'Unione europea[152], rispetto al numero di persone coinvolte che «*will increase by approximately 28% by 2020 and 57% by 2025*»[153].

Inoltre, il sistema può essere impiegato sia come strumento per riconoscere i sospettati anonimi o i responsabili e le vittime di reato, sia come *tool* di *intelligence* per ricostruire il viaggio di un soggetto sospettato di aver commesso una fattispecie di reato[154]. Da qui, emergono espressamente le preoccupazioni del Garante europeo, il quale ha definito come "*unacceptable*" l'impiego di EES per finalità di polizia dal momento che esso è stato concepito eclusivamente come «*a border management tool purely designed with this purpose in mind*»[155].

2. Il volto nell'attuale impianto codicistico italiano

Posto che il volto costituisce una caratteristica fondamentale attraverso cui è possibile riconoscere un soggetto individuato[156], giova ora analizzare brevemente gli istituti processuali interessati dall'accertamento basato su questa tipologia di tratto. Più nel dettaglio, occorre distinguere tra le due attività processuali dell'"'*identikit*" e del "riconoscimento facciale". Mentre nel primo caso le tecniche più all'avanguardia permettono la ricostruzione dell'immagine tridimensionale del volto, nel secondo esse consentono un confronto automatizzato tra l'immagine del soggetto, anche estrapolata dalle

[151] Cfr. il regolamento (UE) 2018/1240. L'ETIAS è stato istituito per imporre ai viaggiatori che entrano in area Schengen, senza la necessità di un visto, di sottoporsi a regole per ottenere un'autorizzazione prima di intraprendere il viaggio qualora possano vi siano rischi per la sicurezza, l'immigrazione illegale o un alto rischio epidemico.

[152] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale,* cit., p. 268 che specifica che «(…) in questa valutazione pesano il numero delle persone coinvolte, la tipologia dei dati processati, le condizioni e i mezzi attraverso cui ciò avviene, il carattere obbligatorio della raccolta, la molteplicità di scopi perseguiti».

[153] Cfr. EUROPEAN COMMISSION, *Impact Assessment Report on the establishment of an EU Entry Exit System*, 6.4.2016, reperibile all'indirizzo https://eur-lex.europa.eu/resource.html?uri=cellar:5c20aef7-fca4-11e5-b713-01aa75ed71a1.0001.02/DOC_2&format=PDF (visualizzato in data 7.12.2021).

[154] V. il considerando n. 26 del regolamento (UE) 2017/2226.

[155] Cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 06/2016 on the Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System*, 21.9.2016, reperibile all'indirizzo https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_en.pdf (visualizzato in data 7.12.2021).

[156] Cfr. il capitolo I, § 3.3.

telecamere di videosorveglianza[157] e le immagini contenute nei *database* nazionali degli organi di polizia[158].

L'elaborazione dell'immagine di un volto, o "*sketch*", presenta un livello di affidabilità piuttosto basso[159]. Posto che l'attività mentale di memorizzazione risulta ricostruttiva e soggetta a continui cambiamenti o interferenze diverse ricerche empiriche hanno dimostrato che la descrizione del volto, frutto delle indicazioni rilasciate dai testimoni o dalla vittima in stato di vulnerabilità, risulta in generale scarsamente aderente a quello originale[160].

La prassi mostra invero una maggiore fiducia verso il riconoscimento dei volti eseguito per mezzo dell'istituto della ricognizione[161]. Come noto, tramite questo mezzo di prova, un soggetto è chiamato a individuare persone, cose, voci, suoni o quanto altro può essere oggetto di percezione sensoriale[162]. Tutti i soggetti possono essere ricognitori attivi e permane l'obbligo di dire la verità. L'imputato poi gode della facoltà di non sottoporsi al compimento dell'atto e l'imputato connesso o collegato può rimanere in silenzio[163]. Dal punto di vista passivo, è discusso se il giudice possa sottoporre coattivamente l'imputato alla ricognizione ed impedire eventuali gesti finalizzati ad evitare il riconoscimento. Lo svolgimento del procedimento è descritto dal codice in modo minuzioso: l'atto può essere compiuto nel corso del dibattimento o durante l'incidente probatorio e si svolge nel contraddittorio tra le parti[164].

Alla tradizionale attività di riconoscimento disciplinata dall'art. 213 c.p.p., si affianca poi la possibilità di utilizzare le immagini estrapolate dai sistemi di videoripresa per sottoporle, come

---

[157] Come più volte ricordato, un dato biometrico digitale può essere il frutto di un procedimento di digitalizzazione, può essere automaticamente generato da un dispositivo IoT ovvero può essere ricavato dalla riproduzione digitale di un dato biometrico trattata da un dispositivo tecnico specifico. Cfr. il capitolo II, § 1.

[158] Cfr. T. Alesci, *Il corpo umano fonte di prova*, Wolters Kluwer, Milano, 2017, p. 90, G. Gulotta, E. M. Tuosto, *Il volto nell'investigazione e nel processo. Nuova fisiognomica forense*, Giuffrè, Milano, 2017, pp. 91 e 109 e ss. e P. Tonini, *Manuale di procedura penale*[13], Giuffrè, Milano, 2012, p. 483.

[159] Tra le tecniche impiegate per l'esecuzione dell'*identikit* o disegno forense vi sono *Identi-Kit*, *Photo-fit*, *E-fit*, *Mac-a-Mug*, *FACES*. Le prime due sfruttano la sovrapposizione di fogli di acetato sui cui sono impresse diverse caratteristiche facciali (per esempio il naso, gli occhi, le sopracciglia, lo stile di capelli, la forma del mento e la forma del volto). Gli altri tre strumenti, invece, sono espressione di una versione moderna e automatizzata dei primi due, producendo un risultato più dettagliato, preciso e realistico. Cfr. G. Gulotta, E. M. Tuosto, *Il volto nell'investigazione e nel processo*, cit., p. 110.

[160] Durante l'esecuzione dell'*identikit* si richiede al testimone di ricordare le singole parti del volto del presunto colpevole nonostante il cervello percepisca la globalità del tratto e non le sue parti specifiche. Peraltro, tale ricostruzione non risulta scevra da condizionamenti esteriori come, per esempio, la pressione psicologica esercitata dalle autorità inquirenti nel tentativo di recuperare il maggior numero di informazioni possibili. Cfr. T. Alesci, *Il corpo umano fonte di prova*, cit., p. 90. V. anche G. Gulotta, E. M. Tuosto, *Il volto nell'investigazione e nel processo,* cit., p. 110 e A. M. Giannini, E. Tizzani, A. D'Amore, L'*identikit*: *come si aiuta un testimone a ricordare*, in *RIC*- 4/2012, p. 284.

[161] Cfr. gli artt. 213 e ss. c.p.p.

[162] Cfr. M. Chiavario, *Diritto processuale penale*[8], Wolters Kluwer, Milano, 2019, pp. 457 e ss.

[163] Cfr. T. Alesci, *Il corpo umano fonte di prova,* cit., p. 91.

[164] Cfr. A. M. Capitta, *Ricognizioni e individuazioni di persone nel diritto delle prove penali*, Giuffè, Milano 2001.

documenti ai sensi dell'art. 234 c.p.p., all'attenzione del testimone o all'analisi dei periti[165]. Trattasi di un meccanismo complesso che si riduce comunque a valorizzare il ricordo mnemonico di un soggetto chiamato, anche a distanza di tempo, a stabilire se una tale persona è la stessa vista in precedenza e in occasione del fatto di reato oggetto del procedimento[166].

L'individuazione, come noto, costituisce invece «un atto tipico del pubblico ministero, delegabile alla polizia giudiziaria»[167]. Tenuto conto della possibilità di ripetere l'atto, la disciplina dell'istituto in esame risulta piuttosto scarna. Peraltro, la suddetta attività di indagine è stata interessata da un'estesa corrente interpretativa giurisprudenziale che gli ha attribuito una natura squisitamente "testimoniale"[168]. Infatti, individuazione e testimonianza risultano due momenti di una medesima operazione probatoria che si snoda fra indagini e dibattimento[169].

Oltre all'individuazione tradizionale, la polizia giudiziaria può altresì compiere un'individuazione fotografica, sia su delega del pubblico ministero, sia di propria iniziativa, in forza del combinato disposto degli artt. 55 e 348 c.p.p. Secondo parte della dottrina, risulta complessa l'indicazione di una cornice normativa entro la quale inserire tale atto atipico d'indagine[170]. Per dar seguito al riconoscimento, il soggetto verrà sottoposto alla consultazione di un album fotografico senza che il procedimento sia scandito temporalmente dall'osservanza di alcun adempimento obbligato. Nonostante l'intrinseca inaffidabilità dei suoi esiti[171], il legislatore rimane comunque consapevole della profonda influenza che le individuazioni possono svolgere nella prima fase d'indagine, essendo questa caratterizzata da ipotesi, approssimazioni e selezioni fra una moltitudine di potenziali responsabili[172].

---

[165] Cfr. A. Bernasconi, *La ricognizione di persone nel processo penale. Struttura e procedimento probatorio*, Giappichelli, Torino, 2003, p. 52. Si veda anche N. Pascucci, *La natura controversa della ricognizione fotografica*, in *RIDPP* fasc.1, 2017, p. 287.

[166] A tal proposito, la prassi giurisprudenziale ha mostrato nel tempo una tendenza a rafforzare la portata applicativa della cd. *ricognizione informale*, cfr. *ex multis* Corte appello L'Aquila, 28.5.2018, n.1269 in *Redazione Giuffrè 2018*; Cass. pen., Sez. IV, 13.9.2017, n.47262 in *CED Cass* n. 271041; Cass. pen., 29.8.2019, n. 37012 in *CED Cass* n. 277635.

[167] Cfr. l'art. 361 c.p.p. V. T. Alesci, *Il corpo umano fonte di prova,* cit., p. 92.

[168] Cfr. *ex multis* Cass. pen., Sez. IV, 25.2.2009, n. 13882 in *CED Cass* n. 243212.

[169] Cfr. T. Alesci, *Il corpo umano fonte di prova*, cit., p. 93. La dottrina ha individuato delle linee guida per la polizia giudiziaria nel compimento di tale attività, cfr. L. D'ambrosio, P. L. Vigna, *La pratica di polizia giudiziaria*, Cedam, Padova, 1998, pp. 304 e 383.

[170] Cfr. *ex multis* Cass. pen., Sez. VI, n. 17747, 15.2.2017 in *CEDCass* n. 269876.

[171] Cfr. S. Priori, *La ricognizione di persona: cosa suggerisce la ricerca psicologica*, in *DPP*, 2003, p. 1284 e S. Priori, *La memoria di riconoscimento nell'atto di ricognizione*, in *DPP*, 2009, p. 775.

[172] Cfr. A. Bernasconi, *Il riconoscimento fotografico curato dalla polizia giudiziaria*, in AA.VV., *Le indagini atipiche*, (a cura di) A. Scalfati, Giappichelli, Torino, 2014, p. 170.

2.1. Il "Sistema Automatico Riconoscimento Immagini" e la rappresentazione digitale dei volti

Entro lo scenario poc'anzi descritto s'inserisce - dal 2017 - l'impiego, da parte degli organi di Polizia, del "Sistema Automatico Riconoscimento Immagini" conosciuto ai più con la sigla del suo acronimo "S.A.R.I."[173]. Un tentativo di ricostruzione delle caratteristiche costitutive e operative di questo «nuovo e, per certi versi, rivoluzionario»[174] strumento può essere operato attraverso il capitolato tecnico[175], allegato al contratto che il Ministero dell'Interno ha sottoscritto con l'azienda privata fornitrice del software[176]. Come specificamente richiesto dal committente, il software è stato predisposto in modo da gestire due scenari operativi, il cd. "*Enterprise*" e il cd. "*Real time*", che coincidono con le modalità applicative poc'anzi descritte (cfr. *supra* il § 1.3). Nella prima, in uso dal settembre 2018, l'operatore ricerca l'identità di un volto presumibilmente raffigurato all'interno di una banca dati di grandi dimensioni individuata nella piattaforma A.F.I.S. – S.S.A. (*Automated fingerprint identification system*)[177], ossia il Sistema automatizzato di identificazione delle impronte digitali integrato dal sottosistema S.S.A. (cfr. il capitolo I, § 3.3.1)[178]. L'immagine fotografica viene così filtrata e processata in pochi istanti con il volto di milioni di soggetti schedati attraverso le impronte facciali elaborate dal software. La procedura di comparazione consente in questo modo di

---

[173] Da qui in avanti "SARI". Per un approfondimento sull'impiego di questo software v. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., pp. 240 e ss., E. Currao, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, cit., pp. 16 e ss., R. Lopez, *La rappresentazione facciale tramite software*, in AA.VV., *Le indagini atipiche*, (a cura di) A Scalfati, Giappichelli, Torino, 2019, pp. 241 e ss., R. Lopez, *Riconoscimento facciale tramite software e individuazione del sospettato*, in AA.VV., *Pre-investigazioni (Espedienti e mezzi)*, (a cura di) A. Scalfati, Giappichelli, Torino, 2020, pp. 297 e ss., J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del Garante Privacy D'Oltremanica)*, in *www.sistemapenale.it*, 28.3.2020, pp. 241 e ss., R.V.O. Valli, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, in *Il Penalista*, 16.1.2019, S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, 2020, pp. 66 e ss. e A. Fonsi, *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time*, in *Penale Diritto e Procedura*, 13.5.2021. Sia consentito il richiamo altresì a E. Sacchetto, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *www.lalegislazionepenale.it*, 16.10.2020. Per vero, sono diversi i Paesi dell'Unione europea che negli ultimi anni si sono dotati di tale strumenti per il perseguimento di 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. Dal 2016, anche le forze di polizia olandesi dispongono del software "CATCH", impiegato per il momento nella sola modalità "a posteriori". Per un approfondimento v. *Towards the European Level Exchange of Facial*
Images - Legal Analysis for TELEFI project, reperibile all'indirizzo https://www.telefi-project.eu/sites/default/files/TELEFI_LegalAnalysis.pdf (visualizzato in data 15.12.2021).

[174] L'espressione è di R. Lopez, *La rappresentazione facciale tramite software*, cit., p. 241.

[175] V. MINISTERO DELL'INTERNO – DIPARTIMENTO DI PUBBLICA SICUREZZA, *Capitolato tecnico, Procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini (S.a.r.i.) lotto n° 1*, reperibile all'indirizzo https://www.poliziadistato.it/statics/06/20160627-ctsari%2D%2D4-.pdf (20.8.2021).

[176] Per maggiori informazioni v. https://www.parsec326.it/ (visualizzato in data 9.12.2021).

[177] Da qui in avanti A.F.I.S.

[178] Peraltro, come sottolinea G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 240, il «sistema (…) in futuro potrà essere integrato con una serie di altre banche dati gestite a livello di Unione europea, ampliando enormemente il volume delle immagini processabili».

ridurre la cerchia dei sospettati grazie all'elaborazione di un elenco di volti selezionati e ordinati per grado di similarità.

Viceversa la modalità cd. "*Real time*", ancora non in uso e finalizzata a potenziare le attività di controllo del territorio in occasione di eventi e manifestazioni, permette l'analisi automatica in tempo reale di volti ripresi in più flussi video *live* provenienti dalle telecamere installate nella medesima area. I volti presenti nei fotogrammi dei diversi *stream* video vengono comparati mediante un algoritmo di riconoscimento che attinge gli elementi della comparazione da una banca dati la cui grandezza è dell'ordine delle centinaia di migliaia di immagini[179]. Una volta inserito il *frame*, il software "passa in rassegna" ad altissima velocità le immagini custodite in archivio e quelle ignote di provenienza eterogenea (sia catturate dallo *streaming* del video, sia riprese da telefoni cellulari) alla ricerca di un *match*. Al termine dell'operazione, l'algoritmo restituisce una lista di profili ordinati secondo un punteggio di probabilità basato sul grado di similarità rispetto all'immagine del soggetto da individuare[180]. La corrispondenza del volto ignoto con quello schedato, come già ricordato *supra*[181], è resa nota all'operatore da un segnale di *alert* generato dall'algoritmo. Se la ricerca non genera alcun *alert*, l'immagine analizzata rimane memorizzata all'interno della piattaforma SARI, così da poter segnalare eventuali corrispondenze future, incrementando in tal modo la possibilità di prossimi *matches*. Se, invece, il tentativo si conclude positivamente, per entrambe le modalità applicative del programma, il risultato dovrà essere posto al vaglio del personale specializzato della polizia scientifica, sul quale incombe il compito di verificare l'esito elaborato dal sistema automatico[182].

A fronte del riserbo tenuto sulle specifiche tecniche di funzionamento del SARI, dal momento che rivelare determinati dettagli «potrebbe alterarne gli esiti investigativi, anche attraverso l'uso di *malware* o software»[183], e delle poche informazioni ricavabili dal capitolato tecnico della gara di appalto per la realizzazione del sistema stesso, la criticità principale rimane quella della completa assenza di un fondamento legislativo che nell'ordinamento italiano disciplini le condizioni di utilizzo di questo strumento. Peraltro, anche l'autorità nazionale Garante per la protezione dei dati personali ha evidenziato la stessa problematica con riferimento al funzionamento di SARI "*Real time*". Vale la

[179] Cfr. R. Lopez, *La rappresentazione facciale tramite software*, cit., p. 243.

[180] Relazione del Dott. L. Rinella, Direttore di Polizia Scientifica durante il convegno "*Dalle impronte digitali al riconoscimento dell'iride: il corpo umano come oggetto e mezzo di investigazione*", organizzato dall'Università del Piemonte Orientale e la Questura di Alessandria, tenutosi ad Alessandria presso il Dipartimento di Giurisprudenza e Scienze politiche, economiche e sociali in data 20 novembre 2019.

[181] V. il § 1.3.

[182] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 241.

[183] Cfr. R. Coluccini, *Lo scontro Viminale-Garante della privacy sul riconoscimento facciale in tempo reale*, in *Irpi*, 13.1.2021, reperibile all'indirizzo https://irpimedia.irpi.eu/viminale-garante-privacy-riconoscimento-facciale-in-tempo-reale/ (visualizzato in data 10.12.2021).

pena a questo punto soffermarsi brevemente sui pareri forniti dal Garante, interpellato sulla legittimità del funzionamento del software in Italia.

2.1.1. Il parere del Garante nazionale sul software nelle due modalità applicative (*real time* vs. *enterprise*)

Con riferimento a SARI "*Enterprise*", al termine della fase di sperimentazione del software, conclusa nel settembre 2018[184], il Garante, con il provvedimento n. 440, ha concluso osservando che «il trattamento di dati personali da realizzarsi mediante il sistema SARI "*Enterprise*", (…), non presenta criticità sotto il profilo della protezione dati»[185]. L'autorità nazionale ha evidenziato come SARI "*Enterprise*", infatti, costituisca solamente uno strumento d'ausilio per l'esecuzione di ricerche all'interno dell'archivio A.F.I.S. ad opera di un addetto che deve comunque inserire manualmente, nella maschera di interrogazione, informazioni anagrafiche, connotati e particolarità di vario genere (per esempio, il colore dei capelli e degli occhi). Entro tale contesto, il software, sottolinea il Garante, si limiterebbe ad automatizzare le operazioni di ricerca e comparazione, consentendo un'elaborazione digitale della ricerca nel database di soggetti precedentemente fotosegnalati, in ogni caso «ferma restando l'esigenza dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato»[186]. Pertanto, secondo il Garante, l'impiego del software «costituisce non un nuovo trattamento di dati personali, (…), bensì un nuova modalità di trattamento di dati biometrici, che dovrà essere effettuata nel rispetto delle regole previste dalla normativa rilevante in materia di tutela dei dati personali»[187]. In particolare, nel provvedimento si specifica che, in conformità all'articolo 7 d.lgs. 51/2018[188], l'impiego di dati personali risulta già previsto e disciplinato da diverse fonti normative e, nello specifico, quelle individuate nel Decreto del Ministro dell'Interno del 24.5.2017. Quest'ultimo ha ad oggetto i diversi trattamenti di dati personali eseguiti dal Centro elaborazione dati del Dipartimento di pubblica sicurezza o da forze di polizia, effettuati con strumenti elettronici, in attuazione dell'art. 53, comma 3, del d.lgs. 196/2003. In particolare, la scheda n. 19 ha ad oggetto il trattamento dei dati personali e identificativi acquisiti dai soggetti sottoposti a

[184] Cfr. MINISTERO DELL'INTERNO, *Comunicato del 19.9.2018*, reperibile all'indirizzo https://www.interno.gov.it/it/notizie/sistema-automatico-riconoscimento-immagini-futuro-diventa-realta (visualizzato in data 10.12.2021).

[185] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell'identità di un volto, n. 440/2018*, 26.7.2018, reperibile all'indirizzo https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9040256 (visualizzato in data 10.12.2021).

[186] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell'identità di un volto, n. 440/2018*, cit.

[187] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell'identità di un volto, n. 440/2018*, cit.

[188] Cfr. il capitolo I, § 1.1.

fotosegnalamento, correlati su base dattiloscopica tramite il sistema A.F.I.S.[189] allocato presso il Servizio polizia scientifica della Direzione centrale anticrimine della Polizia di Stato. Vengono a tal proposito menzionati l'art. 4 TULPS[190] e l'art. 7 del relativo regolamento di esecuzione[191], l'art. 349 c.p.p.[192], l'art. 11 del d.l. 59/1978[193] e l'art. 5 del d.l. 286/1998[194]. Pertanto, il Garante ha ritenuto sufficiente la base normativa già esistente per A.F.I.S. per autorizzare l'attività di trattamento[195].

A distanza di circa tre anni, l'Autorità Garante ha avuto modo di esprimersi anche sulla seconda modalità applicativa di SARI, ossia quella "*Real time*"[196]. Posto quanto stabilito dall'articolo 23 del d.lgs. 51/2018[197], con riferimento alla documentazione prodotta dal Ministero avente ad oggetto la descrizione dei trattamenti nonché la presunta normativa di riferimento indicata all'interno della valutazione d'impatto del sistema, il Garante ha avuto modo di eseguire diverse riflessioni. In primo luogo, l'articolo 1 TULPS disciplina in generale le funzioni dell'Autorità di pubblica sicurezza[198],

[189] Cfr. *supra* il § 2.1 e il capitolo I, § 3.3.1.

[190] Approvato con regio decreto n. 773/1931. L'articolo 4 statuisce che «l'autorità di pubblica sicurezza ha facoltà di ordinare che le persone pericolose o sospette e coloro che non sono in grado o si rifiutano di provare la loro identità siano sottoposti a rilievi segnaletici. Ha facoltà inoltre di ordinare alle persone pericolose o sospette di munirsi, entro un dato termine, della carta di identità e di esibirla ad ogni richiesta degli ufficiali o degli agenti di pubblica sicurezza».

[191] Approvato con regio decreto n. 635/1940. L'articolo 7 dispone che «i rilievi segnaletici per le persone pericolose o sospette e per coloro che non siano in grado o si rifiutino di provare la propria identità, giusta l'art. 4 della Legge, sono descrittivi, fotografici, dattiloscopici e antropometrici. La carta d'identità da rilasciarsi alle persone pericolose o sospette, a termini del citato art. 4, deve essere conforme al modello allegato al presente regolamento, senza particolari rilievi od annotazioni. Le impronte digitali sono apposte sui cartellini da conservarsi presso l'ufficio comunale e l'ufficio provinciale di pubblica sicurezza». V. il capitolo I, § 2.

[192] V. il capitolo I, § 2.

[193] Convertito in legge n. 191/1978. L'articolo 11 dispone che «gli ufficiali e gli agenti di polizia possono accompagnare nei propri uffici chiunque, richiestone, rifiuta di dichiarare le proprie generalità ed ivi trattenerlo per il tempo necessario all'identificazione o comunque non oltre le ventiquattro ore. La disposizione prevista nel comma precedente si applica anche quando ricorrono sufficienti indizi per ritenere la falsità delle dichiarazioni della persona richiesta sulla propria identità personale o dei documenti d'identità da essa esibiti. Dell'accompagnamento è data immediata notizia al procuratore della Repubblica, il quale, se riconosce che non ricorrono le condizioni di cui al comma precedente, ordina la liberazione della persona accompagnata».

[194] Il testo della norma è reperibile all'indirizzo https://www.camera.it/parlam/leggi/deleghe/98286dl.htm (visualizzato in data 10.12.2021).

[195] V. su questo punto G. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *www.lalegislazionepenale.it*, 11.12.2021, p. 5.

[196] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time - 25 marzo 2021*, n. 127, reperibile all'indirizzo https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877 (visualizzato in data 13.12.2021).

[197] «Se il trattamento, per l'uso di nuove tecnologie e per la sua natura, per l'ambito di applicazione, per il contesto e per le finalità, presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima di procedere al trattamento, effettua una valutazione del suo impatto sulla protezione dei dati personali. 2. La valutazione di cui al comma 1 contiene una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e il rispetto delle norme del presente decreto». Il testo del decreto è reperibile all'indirizzo https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario (visualizzato in data 13.12.2021).

[198] L'articolo 1 TULPS stabilisce che l'autorità di pubblica sicurezza ha la funzione di mantenere l'ordine pubblico, la sicurezza dei cittadini e la loro incolumità, nonché tutelare la proprietà. Essa cura inoltre l'osservanza delle leggi e dei regolamenti generali e speciali dello Stato, delle province e dei comuni, nonché delle ordinanze delle autorità. I commi 2, 3 e 4 specificano poi che «per mezzo dei suoi ufficiali, ed a richiesta delle parti, provvede alla bonaria composizione dei dissidi privati. L'autorità di pubblica sicurezza è provinciale e locale. Le attribuzioni dell'autorità provinciale di pubblica sicurezza sono esercitate dal prefetto e dal

senza operare alcun riferimento al trattamento di dati biometrici. Parimenti, gli articoli 134 comma 4, 234, 266 e 431 comma 1, lett. *b)* c.p.p. – aventi ad oggetto la documentazione degli atti per riproduzione audiovisiva, l'acquisizione di documenti mediante fotografia ed altri mezzi e l'intercettazione di flussi di comunicazioni telematiche o tra presenti mediante dispositivi elettronici portatili – non possono costituire una pertinente base giuridica per il trattamento di dati biometrici finalizzato all'identificazione dell'individuo in modalità "*live*".

Ancora, gli artt. 55, 348, 354 e 370 c.p.p., concernenti le funzioni di polizia giudiziaria aventi ad oggetto la tutela delle fonti di prova e degli accertamenti su luoghi o persone, di iniziativa o su delega dell'Autorità giudiziaria, nulla dicono circa il trattamento dei dati biometrici. Infine, il d.P.R. 15.1.2018, n. 15, recante la disciplina del trattamento dei dati effettuato per le finalità di polizia include altresì l'impiego dei dati attraverso i sistemi di videosorveglianza e di ripresa fotografica, audio e video, «sistemi ontologicamente diversi da quelli dei dati biometrici»[199].

Alla luce di quanto precede, pertanto, secondo il Garante, le suddette disposizioni non risultano idonee per il soddisfacimento dei requisiti di specificità richiesti dall'articolo 23 per il trattamento dei dati biometrici per finalità di sicurezza pubblica e repressione dei reati; articolo che, tra l'altro, «non può considerarsi, di per sé, fonte normativa idonea a legittimarli, in quanto è diretto a specificare le condizioni che ne consentono l'effettuazione, tra le quali individua, appunto, la sussistenza di una norma del diritto dell'Unione o dello Stato nazionale che lo autorizzi specificamente». Non è pertanto possibile, allo stato attuale, individuare alcuna base giuridica, ai sensi dell'articolo 7 d.lgs. 51/2018, che sia idonea a consentire il trattamento dei dati biometrici per le finalità in argomento. La modalità applicativa "*Real time*" di SARI, secondo il Garante, determinerebbe un'attività di sistematica sorveglianza di massa che consentirebbe di generare e trattare, senza alcuna specifica normativa di riferimento, le rappresentazioni digitali dei volti di una moltitudine di consociati al fine di confrontarli con quelle dei soggetti inseriti nella *watch-list* di riferimento (cfr. *supra*, il § 1.3)[200].

---

questore; quelle dell'autorità locale dal capo dell'ufficio di pubblica sicurezza del luogo o, in mancanza, dal Podestà». Il testo della norma è reperibile all'indirizzo https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1931-06-18;773!vig= (visualizzato in data 13.12.2021).

[199] Il parere del Garante rimanda al considerando n. 51 del regolamento (UE) 2016/679 (cfr. il capitolo I, § 1). In ogni caso è bene ricordare che, nonostante la modalità "*Real-time*" del software abbia ricevuto un parere negativo del Garante, l'art. 160-*bis*, inserito nel d.lgs. 30 giugno 2003, n. 196 (c.d. "codice della privacy") dal d.lgs. 10 agosto 2018, n. 101, prevede che «la validità, l'efficacia e l'utilizzabilità el procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento restano disciplinate dalle pertinenti disposizioni processuali».

[200] Cfr. altresì GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sulla valutazione di impatto del Ministero dell'Interno relativo ad un sistema di telecamere indossabili (body-cam), da Reparti mobili della Polizia di Stato, per la documentazione audio e video di situazioni critiche per l'ordine e la sicurezza, in occasione di eventi o manifestazioni pubbliche*, 22.7.2021, p. 7, reperibile all'indirizzo https://www.asaps.it/downloads/files/Garante%20Privacy%20provvedimento%20bodycam%20Polizia%20di%20Stato%20luglio%202021.pdf (visualizzato in data 14.12.2021), con cui si è escluso che i dispositivi in questione possano essere impiegati in funzione di «identificazione univoca […] o autenticazione di

Invero, proprio alla luce delle argomentazioni a sostegno del parere negativo rilasciato dal Garante sulla modalità "*Real time*", sorgono alcuni dubbi interpretativi in seno alla normativa individuata per SARI "*Enterprise"*. Il combinato disposto degli artt. 4 TULPS e 7 del relativo regolamento di esecuzione, del 349 c.p.p., dell'art. 11 del d.l. 59/1978 e l'art. 5 del d.l. 286/1998, individuati come base normativa di riferimento per la modalità applicativa in "*post remote*" di SARI può realisticamente considerarsi sufficientemente dettagliato nella sua attuale formulazione? Il generico riferimento alla possibilità di fotosegnalare o eseguire rilievi fotografici, antropometrici ovvero eseguire "altri accertamenti" nei confronti di un soggetto ritenuto pericoloso o sospettato può considerarsi idoneo per il soddisfacimento dei requisiti di specificità, richiesti *ut supra* dall'articolo 7, per il trattamento dei dati biometrici, per il perseguimento di finalità di sicurezza pubblica e repressione dei reati? Da una parte, la genericità delle formule contenute nelle succitate disposizioni normative consentirebbe l'adeguamento delle norme alle innovazioni scientifiche tra le quali potrebbero annoverarsi anche quelle in esame, dall'altra, come anticipato *supra*[201], l'espressione costituisce un veicolo per potenziali e molteplici strumenti atipici di indagine che assegnano alla polizia giudiziaria «margini non trascurabili di discrezionalità operativa»[202].

2.1.2. Il fenomeno delle "*smart cities*": i progetti pilota di Como, Torino e Venezia

A titolo esemplificativo si ritiene utile richiamare brevemente alcuni progetti pilota messi a punto dai Comuni di Como, Torino e Venezia[203]. A riprova, infatti, della difficoltà - evidenziata con il provvedimento poc'anzi descritto dal Garante per la protezione dei dati personali - di individuare una base normativa idonea per l'impiego della modalità applicativa "*real time*" dei sistemi di riconoscimento facciale, vi è una recente decisione - seppur precedente al parere n. 127/2021- dello stesso Garante che ha da poco inibito al Comune di Como l'impiego di sistemi di videosorveglianza integrati con la tecnologia di riconoscimento facciale a scopo di indagine e di prevenzione nell'ambito delle politiche di sicurezza urbana[204]. Il Comune, infatti, aveva predisposto siffatte misure in base alla

una persona fisica (*facial recognition*)».

[201] Cfr. il capitolo III, § 1.3.1.

[202] Cfr. T. Alesci, *Corpo dell'imputato (fonte di prova nel processo penale)*, in *Digesto delle Discipline Penalistiche*, Utet, Milano, 2018, p. 81.

[203] L'espressione "*Smart cities*" si riferisce alle città che impiegano «*new technologies, such as AI and big data analytics, for various applications, such as transportation, trash collection, street repairs, administrative efficiency, surveillance, and more*». M. Ziosi, B. Hewitt, P. Juneja, M. Taddeo, L. Floridi, *Smart Cities: Mapping their Ethical Implications*, 5.1.2022, reperibile all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4001761 (visualizzato in data 15.1.2022). V. su questo anche R. Kitchin, *The real-time city? Big data and smart urbanism*, in *GeoJournal*, 79, pp. 1-14.

[204] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 26 febbraio 2020, n. 54*, reperibile all'indirizzo https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9309458 (visualizzato in data 14.12.2021).

normativa che consente l'impiego di impianti di videosorveglianza nel contesto urbano[205], la quale, tuttavia, non autorizza espressamente il trattamento di dati biometrici[206], come invece richiesto dall'articolo 7 del già richiamato d.lgs. n. 51/2018[207]. Pertanto, non essendo rinvenibile alcuna base normativa idonea a giustificare l'impiego di tale tecnologia, l'Autorità Garante, ai sensi dell'art. 37, comma 3, lettera *d),* del d.lgs. 51 del 2018, ha invitato il Comune a conformarsi rispetto a quanto prescritto dal decreto stesso, inibendo così la possibilità di impiegare tale specifica modalità applicativa.

Entro tale contesto e, nonostante il Garante nazionale - come visto *supra* - avesse rilasciato nel frattempo al Ministero dell'Interno un parere negativo per l'impiego di tecniche di riconoscimento facciale per finalità di prevenzione e sicurezza in contesti urbani, alcune città, tra le quali Torino e Venezia, valutavano l'inserimento di questa particolare tipologia di software nelle telecamere installate per la videosorveglianza degli spazi pubblici. Ed è questo il caso del progetto ARGO che, a poco meno di un mese di distanza dal provvedimento n. 127/2021[208], veniva confermato dal Comune di Torino. Con questa iniziativa, si è proposto, al fine di controllare la sicurezza urbana, la sicurezza integrata e la *governance* della mobilità, di potenziare una rete di videosorveglianza diffusa, in aggiunta alle videocamere già installate precedentemente, aventi funzioni di *crossing detection* (rilevazione del superamento di una linea predefinita), *intrusion detection* (rilevazione di intrusioni in una certa area), *region entrance* (rilevazione dell'entrata di una persona/veicolo in una regione predefinita), *region exiting* (il contrario della precedente) e *motion detection* (rilevazione del

[205] Cfr. il capitolo III, § 2.4, nota n. 387. Cfr. la l. 23.4.2009 n. 38, art. 6, commi 7 e 8, sulla utilizzabilità, da parte dei Comuni, di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana. Cfr. COMUNE DI COMO, *Documento unico programmatico 2020-2022*, reperibile all'indirizzo https://www.comune.como.it/export/sites/default/it/comune/bilanci-documenti-piani/documento-unico-programmazione/DUP-2020-2022.pdf (visualizzato in data 13.12.2021) in cui, *inter alia*, si programmava «la "*remise-en-forme*" dell'attuale sistema di videosorveglianza comunale, prevedendo, tra l'altro, una più efficace sistemazione della sala operativa della Polizia Locale [e] (…) una postazione di controllo remoto del sistema di videosorveglianza comunale. Si individueranno in accordo con la PL nuove aree sensibili da sottoporre al controllo di videocamere. La zona dei giardini di viale Tokamachi sarà interessata da un "progetto pilota" per la sperimentazione di funzioni innovative di videosorveglianza, quali *face recognition*, *loitering*, e rilevamento automatico abbandono/furto di oggetti. La sperimentazione comporta anche la definizione dei rapporti con le altre forze di polizia sia in termini di protocolli di utilizzo che di accesso tecnologico al sistema, nonché, ovviamente, la definizione delle regole di utilizzo conformi al GDPR».

[206] Le disposizioni normative richiamate dal Comune di Como «si limitano infatti, in particolare, a consentire l'identificazione dell'indagato e delle persone in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti (art. 349 c.p.p.), a indicare le modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia (d.P.R. n. 15/2018), ovvero a legittimare l'installazione di videocamere per fini di tutela della sicurezza urbana e comunque in assenza della specifica previsione normativa della raccolta di dati biometrici (art. 6, comma 7, d.l. n. 11/2009), necessaria ai sensi dell'art. 7 d.lgs. n. 51/2018». GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 26 febbraio 2020*, n. 54, cit.

[207] V. il § precedente e il capitolo I, § 1.1.

[208] V. http://www.comune.torino.it/circ7/cm/pages/ServeBLOB.php/L/IT/IDPagina/6837 (visualizzato in data 22.1.2022).

movimento di una persona/veicolo)[209]. Le fasi del progetto sarebbero essenzialmente due: in primo luogo, l'operazione coinvolgerebbe l'area periferica, nella quale confluisce l'attività di gestione dei sistemi di videosorveglianza realizzata nell'ambito del progetto "AxTO"[210]; successivamente, il piano è quello di coinvolgere l'area centrale della città[211]. Le videocamere, in questo caso, a differenza del progetto del Comune di Como, non sono in grado di riconoscere i volti delle persone, ma di categorizzare le medesime in base al genere e agli indumenti indossati, ovvero di individuare la presenza di oggetti (per esempio cappelli, zaini e borse), ossia di estrarre i cd. "metadati"[212]. La tecnologia in esame sarebbe pertanto in grado di monitorare costantemente gli spostamenti delle persone e prendere nota del loro aspetto e dove sono collocate, ma non di eseguire dei veri e propri riconoscimenti. In questo caso, il Garante nazionale ha ritenuto opportuno aprire un'istruttoria preliminare al fine di analizzare e comprendere la *ratio* di tale progetto[213]. Il rischio è quello - *inter alia* - di collezionare una serie di dati classificando gli individui in base a categorie standard e potenzialmente discriminatorie, tenendo conto soprattutto che diversi studi empirici hanno dimostrato che anche gli algoritmi più avanzati commettono degli errori nella distinzione tra identità di genere e sesso biologico[214].

Un altro esempio paradigmatico è quello del Comune di Venezia. Il sistema, messo a punto nell'ambito del progetto "*Smart Control Room*"[215], è costituito da un *server* in grado di aggregare e controllare telecamere dotate di una tecnologia che permette di prevedere gli eventi metereologici, definendo percorsi alternativi per il transito nella città, indicare alla popolazione in tempo reale i percorsi da evitare per il traffico, gestire la mobilità ottimizzandone i tempi, controllare l'occupazione dei parcheggi e monitorare costantemente l'afflusso dei visitatori. Anche in questo caso, sono stati

[209] Cfr. L. Carrer, *La soluzione "innovativa" di Torino*, 28.1.2021, reperibile all'indirizzo https://www.hermescenter.org/la-soluzione-innovativa-di-torino-argo/ (visualizzato in data 14.12.2021).

[210] Cfr. https://servizi.comune.torino.it/consiglio/prg/web/scheda_atto.php?c_argomento=I202100288 (visualizzato in data 14.12.2021). V. anche CITTÀ DI TORINO, *AxTO - Azioni per le periferie torinesi*, reperibile all'indirizzo http://www.comune.torino.it/arredourbano/bm~doc/relazione-generale-axto.pdf (visualizzato in data 14.12.2021).

[211] Il progetto è stato reso definitivo a ottobre 2020. Cfr. L. Carrer, *La soluzione "innovativa" di Torino*, 28.1.2021, cit.

[212] Cfr. il capitolo I, § 2.4.

[213] Anche sulla base dell'interpretazione fornita dall'*European Data Protection Board* secondo il quale «*"identification" does not need to reveal someone's official name or identity, but includes any processing that makes it possible to distinguish one person from others, which can be equally intrusive*». EDPB, *Guidelines 3/2019 on processing of personal data through video devices* (2019) 16 https://edpb.europa.eu/sites/edpb/ files/consultation/edpb_guidelines_201903_videosurveillance.pdf (visualizzato in data 14.12.2021).

[214] Cfr. M. Millar, *Facial recognition technology struggles to see past gender binary*, 30.10.2019, reperibile all'indirizzo https://www.reuters.com/article/us-usa-lgbt-facial-recognition/facial-recognition-technology-struggles-to-see-past-gender-binary-idUSKBN1X92OD?edition-redirect=uk (visualizzato in data 14.12.2021).

[215] Cfr. E. Mureddu, *Come Venezia è diventata il grande fratello d'Europa*, 27.10.2021, reperibile all'indirizzo https://europa.today.it/attualita/venezia-grande-fratello.html (visualizzato in data 14.12.2021) e GREENS/EFA IN THE EUROPEAN PARLIAMENT, *Biometric Behavioural Mass Surveillance in EU Member States*, Ottobre 2021, reperibile all'indirizzo http://extranet.greens-efa.eu/public/media/file/1/7297 (visualizzato in data 14.12.2021).

sollevati alcuni dubbi circa l'effettiva legittimazione della predisposizione e dell'impiego sistematico di siffatti strumenti[216].

Per tale ragione, contestualmente all'introduzione delle iniziative poc'anzi descritte, veniva presentato un disegno di legge volto a sospendere l'impiego delle tecnologie in questione[217]. Nel preambolo, in particolare, si specificava che, considerato come risultino «ormai molti i comuni italiani, compresi i grandi capoluoghi, che progettano di trasformare i loro sistemi di videosorveglianza in veri e propri sistemi di riconoscimento facciale» e, pur «in assenza di un quadro normativo che consenta di uniformare le condizioni per l'utilizzo dei dati biometrici da parte degli enti territoriali, in particolare per le funzioni di polizia giudiziaria riservate alla polizia locale», il disegno di legge proponeva di introdurre una «moratoria dell'utilizzo dei sistemi di riconoscimento facciale nei luoghi pubblici o aperti al pubblico […] fino a quando non sarà adottata una normativa che assicuri il pieno rispetto dei diritti costituzionali dei cittadini, conformemente alle indicazioni delle autorità nazionali ed europee per la protezione dei dati personali». Oltre a ciò, l'articolo 1 del d.d.l. stabiliva l'effettiva sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale, «fino all'entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2021».

Tale iniziativa si è effettivamente tradotta in legge, con l'introduzione del d.l. 139/2021 (cd. decreto "Capienze") convertito con modificazioni dalla l. 205/2021[218]. Tuttavia, non si comprende a fondo la *ratio* dell'intervento, alla luce di quanto stabilito in sede di disegno di legge. Più nel dettaglio, l'art. 1, co. 9 dispone che «l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici di cui all'articolo 4, numero 14), del citato regolamento (UE) 2016/679 in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, sono sospese fino all'entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2023»[219]. Tale moratoria però non si applica «ai trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di

[216] Giova fare cenno altresì del caso del Comune di Udine, ove è stata solamente annunciata la volontà di installare un nuovo sistema di videosorveglianza, con 67 nuove telecamere, in aggiunta alle 75 già presenti nella città e agli 11 sistemi di lettura delle targhe dei veicoli. La proposta è quella di implementare gli strumenti di video-analisi, come il riconoscimento di mezzi e individui in base ad una serie di criteri come, per esempio, l'età, il sesso, gli abiti, l'orario, attraverso l'impiego di software di analisi forense. Cfr. https://www.ilgiornalediudine.com/cronaca/green-pass-e-riconoscimento-facciale-udine-punta-a-un-sistema-di-sorveglianza-cinese/ (visualizzato in data 14.12.2021).

[217] Cfr. il d.d.l. AC 3009, "*Sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici in luoghi pubblici o aperti al pubblico*", 12.4.2021, reperibile all'indirizzo http://documenti.camera.it/leg18/pdl/pdf/leg.18.pdl.camera.3009.18PDL0137680.pdf.

[218] Cfr. il d.l. 139/2021 convertito con modificazioni dalla l. 205/2021 "*Disposizioni urgenti per l'accesso alle attivita' culturali, sportive e ricreative, nonché' per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali*" reperibile all'indirizzo https://www.gazzettaufficiale.it/eli/id/2021/10/08/21G00153/sg.

[219] Cfr. l'art. 9 co. 11 d.l. 139/2021.

esecuzione di sanzioni penali di cui al decreto legislativo 18 maggio 2018, n. 51, in presenza, salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero, di parere favorevole del Garante reso ai sensi dell'articolo 24, comma 1, lettera b), del medesimo decreto legislativo n. 51 del 2018»[220].

In primo luogo, occorre riflettere sul fatto che nella nozione di "autorità competenti a fini di prevenzione e repressione dei reati" rientrano altresì le pubbliche amministrazioni[221]. Questo significa che i Comuni, o meglio, ciascun ente pubblico incaricato di esercitare poteri a fini di prevenzione, indagine è autorizzato a servirsi di impianti di videosorveglianza dotati di software di riconoscimento facciale senza dover attendere la predisposizione di una compiuta disciplina legislativa in materia.

La *ratio* di tale disposizione risulta completamente antitetica rispetto alla preoccupazione manifestata nel preambolo del d.d.l. Infatti, con l'entrata in vigore del d.l. 139/2021, gli enti territoriali, in seguito ad un parere favorevole del Garante, potranno installare i loro sistemi di videosorveglianza dotati di tecnologie di riconoscimento facciale e attivarli in spazi aperti al pubblico. Ma allora quale può essere l'effettiva *intentio legis*, se l'assenza di uno specifico quadro normativo di riferimento era proprio la ragione per la quale si era proposta una sospensione dell'impiego di tali *tools*?

In secondo luogo, dalla stessa moratoria si esclude l'impiego dei software di riconoscimento facciale da parte dell'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali e del pubblico ministero[222]. Il testo normativo, non distinguendo fra modalità "in tempo reale" e "in differita", sembra riferirsi ad un ricorso indiscriminato del software a fini giudiziari che genera non poca confusione. Questo potrebbe senz'altro comportare diverse problematiche interpretative e applicative se si considera che la normativa codicistica non contiene alcun dettaglio o specifica tecnica per l'impiego di tali strumenti (v. *infra* i §§ 2.3 e ss.).

2.3. *Facial recognition technology* e processo penale in Italia

Senza dubbio, attraverso l'impiego del software in parola, sia esso utilizzato per eseguire riconoscimenti "in tempo reale" ovvero "a posteriori"[223], il vantaggio per il lavoro degli operatori di polizia di sicurezza e giudiziaria risulta evidente, sia sul piano della velocità, sia su quello dell'efficienza. Si consideri solo che, fino a pochi anni fa, l'esecuzione della ricerca informatizzata al

[220] Cfr. l'art. 9 co. 12 d.l. 139/2021.

[221] Cfr. la definizione di "autorità competente" contenuta nell'art. 3 par. 7 LED che include «*a)* qualsiasi autorità pubblica competente in materia 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; o *b)* qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica».

[222] Cfr. l'art. 9 co. 12 d.l. 139/2021.

[223] Cfr. *supra* il § 1.3.

tempo in uso imponeva che i connotati identificativi del soggetto, i dati anagrafici e somatici, fossero indicati in forma descrittiva e inseriti manualmente dall'operatore nei campi presenti nelle maschere di interrogazione[224].

Dal punto di vista processuale penale, il software può trovare applicazione sia nella fase delle indagini preliminari sia, in seguito, in fase dibattimentale. Ed invero, si è opportunamente rimarcato come la tendenza pressoché costante sia quella di qualificare tali attività «alla stregua di mezzi atipici ma nel contempo legittimi di ricerca probatoria»[225].

2.3.1. Dalle indagini preliminari…

Con riferimento alla fase delle indagini, l'impiego di S.A.R.I. "*Enterprise*" è destinato ad affermarsi nel vasto filone di tecniche inedite che l'inarrestabile sviluppo scientifico degli ultimi anni ha prodotto e di cui fanno parte diversi strumenti, entro l'ampia categoria delle "indagini atipiche"[226]. L'espressione evoca una nozione «sfumata»[227] e, forse, non così adeguata a fornire i contorni precisi di tale tipologia di atti, data la pluralità delle attività che contiene al suo interno. La tendenza da parte delle autorità inquirenti è quella di ricorrere a tali strumenti di indagine non solo per l'efficacia e l'estrema velocità dei risultati, ma, certamente, anche per l'indeterminatezza dei limiti all'azione investigativa. In ogni caso, l'attività rientrerebbe tra i compiti istituzionali della polizia giudiziaria finalizzati ad assicurare le fonti di prova e quant'altro possa servire per l'applicazione della legge penale attraverso la ricerca di ogni elemento utile alla ricostruzione del fatto e alla individuazione del colpevole ai sensi del combinato disposto degli artt. 55 e 348 c.p.p. In particolare, S.A.R.I. "*Enterprise*" è ad oggi impiegato dalla polizia giudiziaria per eseguire solamente una prima macro ricerca nel database A.F.I.S.-S.S.A. fra i soggetti precedentemente foto segnalati[228]. L'*outcome* scaturente dal software risulta così utile durante la prima fase delle indagini per il fine esclusivo di operare una scrematura fra più possibili direzioni di investigazione.

Il risultato di *match* o *non-match* espresso in percentuale è poi nella prassi affidato al personale specializzato di polizia scientifica, sul quale incombe il compito di validare l'esito elaborato dal sistema automatico, attraverso il tradizionale metodo di comparazione fisionomico[229]. Ciò in ragione del fatto che, come nel caso dei software di comparazione automatica delle impronte digitali, i sistemi

[224] Cfr. R. Lopez, *La rappresentazione facciale tramite software,* cit., p. 243.
[225] Cfr. D. Negri, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, 2020, f. 1, p. 26.
[226] Cfr. il capitolo III, § 1.1.2.
[227] Aggettivo utilizzato da A. Scalfati, *Premessa*, in AA.VV., *Le indagini atipiche*, (a cura di) A. Scalfati, Giappichelli, Torino, 2014, p. 15.
[228] Cfr. *supra* il § 2.1.
[229] Cfr. R. Lopez, *Riconoscimento facciale tramite software e individuazione del sospettato*, cit., p. 301.

di riconoscimento facciale attualmente in uso alle forze di polizia non sono in grado di calcolare il rapporto fra similarità e tipicità del dato rispetto ad una popolazione di riferimento (cd. "rapporto di verosimiglianza") [230]. Il programma è, infatti, in grado di stimare solamente la *similarità* dei campioni posti a confronto, ma non la *tipicità* ossia quanto il campione in esame sia comune in una determinata parte della popolazione. Per tale ragione, il risultato di compatibilità o meno, scaturente dal software, sarà solo parziale, corrispondente ad un calcolo di coincidenza delle misure fra i diversi punti di repere[231]. Come visto *supra*[232], per acquisire un legame, seppur di "secondo grado", con il *thema probandum*, è necessario un confronto manuale eseguito da un operatore esperto, il quale applicherà una metodologia di comparazione/misurazione conforme agli standard e alle procedure elaborati dalla comunità scientifica di riferimento, atte a stabilire se due modelli elettronici dello stesso tratto biometrico appartengano effettivamente o meno alla stessa persona. Su questo aspetto, tuttavia, potrebbero in ogni caso sorgere alcuni dubbi circa l'effettiva capacità del giudice nel valutare comunque il giudizio formulato dall'esperto e l'attendibilità sulla specifica metodologia impiegata[233].

2.3.2 …alla corrispondenza automatica tra tipicità e atipicità probatoria

Rispetto, invece, alla fase dibattimentale si ritiene opportuno muovere dalle distinzioni operate *supra*, aventi ad oggetto la diversa natura delle rappresentazioni digitalizzate dei tratti coinvolti in una data comparazione automatica tramite software[234]. Come già più volte ricordato[235], infatti, un dato biometrico può trovarsi sotto forma di rappresentazione digitalizzata del tratto o del suo relativo *template*; può essere ricavato da un'immagine o da un video trattati da un "dispositivo tecnico specifico"[236]; può derivare da dati elaborati automaticamente per un uso generico o commerciale e quindi estranei al procedimento penale. Orbene, il *match* scaturente da sistemi automatizzati di riconoscimento impiegati comparando le *features* ricavate da un'immagine digitale attraverso

[230] Su questo punto v. *Best Practice Manual for Facial Image Comparison*, pubblicate dall'ENFSI-BPM-DI-01 Version, 01 - January 2018, reperibili all'indirizzo https://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf, T. Bove, P. E. Giua, A. Forte, C. Rossi, *Un metodo statistico per il riconoscimento del parlatore basato sull'analisi delle formanti*, in *Statistica*, anno LXII, n. 3, 2002, p. 480, C. Aitken, F. Taroni, *Statistics and the Evaluation of Evidence for Forensic Scientists*, Wiley, New York, 2004, C. Aitken, R. Roberts, G. Jackson, *Fundamentals of probability and statistical evidence in criminal proceedings: guidance for judges, lawyers, forensic scientists and expert witnesses*, Royal Statistical Society, London, 2010, D.H. Kaye, *Statistics for lawyers and law for statistics*, in *89 Mich. L. Rev.*, 1991, p. 1520.

[231] Cfr. *supra* il § 1.

[232] Cfr. il capitolo III, § 1.3.

[233] Cfr. P. De Hert, *Biometrics: legal issues and implications*, in *Background paper for the Institute of Prospective Technological Studies*, DG JRC – Sevilla, European Commission, 2005, p. 39.

[234] Cfr. il capitolo II, § 1.

[235] Cfr. il capitolo II, § 1.

[236] Cfr. il capitolo I, § 1.

procedimenti di digitalizzazione risulta, come già anticipato *supra*[237], per prassi, sempre soggetto ad un confronto manuale da parte di un operatore esperto[238], il quale è tenuto a seguire le metodologie di misurazione manuali, conformi agli standard e alle procedure elaborate dalla comunità scientifica di riferimento[239]. Spetta, infatti, agli esperti forensi comparare manualmente le due immagini per determinare il valore esatto di compatibilità fra le stesse[240]. Quanto ai metodi di riconoscimento dei volti applicati in via manuale dagli operatori, si sono succeduti nel tempo diversi approcci che si richiamano brevemente qui di seguito[241].

Comparazione olistica	I volti sono confrontati simultaneamente 1:1. Uno dei metodi olistici più utilizzati è *Eigenfaces*. Tale approccio consta di cinque fasi. La prima di queste prevede l'inserimento di una serie di immagini all'interno di un database (cd. *training set*). La seconda fase prevede la creazione delle cd. *eigenfaces*, estraendo gli elementi caratteristici dei volti. Le immagini sono normalizzate al fine di allineare gli occhi e la bocca. Le immagini vengono poi ridimensionate in modo tale che abbiano la stessa grandezza. A questo punto, durante la terza fase, ogni *eigenface* sarà rappresentata come un "vettore di pesi". Una volta inserita la *query* nel sistema, se il peso dell'immagine di ingresso risulta superiore ad una certa soglia, allora la si considera coincidente con quella di riferimento. L'immagine nel database con il peso più vicino sarà restituito all'utente del sistema come risultato.
Foto Antropometria	Tale approccio si basa sulla misura spaziale delle caratteristiche facciali, le distanze e gli angoli tra i punti di riferimento del volto[242].

[237] Cfr. il capitolo III, § 1.3.

[238] Ai sensi degli artt. 220 e 233 c.p.p. Su questo punto v. E. Currao, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, cit., p. 21.

[239] Cfr. ENFSI, *Best Practice Manual for Facial Image Comparison*, 2018, reperibile all'indirizzo https://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf (visualizzato in data 21.12.2021).

[240] Nel settore del riconoscimento facciale sono attivi numerosi gruppi di lavoro che si occupano di standardizzare il procedimento di confronto manuale 1:1 e di fornire una corretta formazione agli esperti forensi tramite la redazione e la condivisione di linee guida. Si ricorda, negli Stati Uniti, il *Facial Identification Scientific Working Group* (FISWG), il *Biometric Center of Excellence* (BCOE) e l'*International Association for Identification*. In Europa, l'*European Network of Forensic Science Institutes* (ENFSI). Su questo punto v. G. Gulotta, E.M. Tuosto, *Il volto nell'investigazione e nel processo. Nuova Fisiognomica Forense*, Giuffrè, Milano, 2017, pp. 120 e ss.

[241] Per un approfondimento v. G. Gulotta, E.M. Tuosto, *Il volto nell'investigazione e nel processo. Nuova Fisiognomica Forense*, cit., pp. 118 e ss. e T. Ali, R. Veldhuis, L. Spreeuwers, *Forensic Face Recognition: A Survey*, in AA.VV., *Face recognition: methods, applications and technology*, (a cura di) A. Quaglia, C. M. Epifano, NOVA Publishers, Enschede, 2010, pp. 9–15

[242] Per un approfondimento v. M. Reuben, J. Morley, *Investigation into the use of photoanthropometryin facial image comparison*, in *Forensic science international*, 212.1 (2011), pp. 231-237 e K. F. Kleinberg, B. Pharm ,P. Vanezis M.D., A.M. Burton, *Failure of Anthropometry as a Facial Identification Technique Using High-Quality Photographs*, in *Journal of Forensic Sciences*, 2007, 52(4), pp. 779 – 783.

Sovrapposizione	La versione in scala della rappresentazione del volto è confrontata con un'altra ed entrambe devono essere analizzate dalla stessa angolazione. Tale tecnica è denominata anche "sovrapposizione parametrizzata" e consiste in una comparazione fisionomica e metrica tra due immagini. La compatibilità fra due volti può dirsi raggiunta quando sussiste una sovrapponibilità tra diversi punti luminosi fissati sul volto del reo (cd. punti di repere) e le forme anatomiche dell'indagato.
Analisi morfologica con classificazione delle caratteristiche	Tramite questo metodo, alcune specifiche caratteristiche individuali sono comparate e classificate. Il confronto si concentra sul contorno delle guance, le linee del mento, la forma della bocca, degli occhi, del naso, delle orecchie, dei nei, delle rughe, delle cicatrici e di particolari segni presenti sul volto.

Schema n. 1

Per quanto concerne invece il *match* o *non-match* automaticamente generato da un dispositivo IoT (per es. uno *smartphone*), si è visto *supra* come esso possa, in alcuni casi, rappresentare un patrimonio conoscitivo fondamentale per il procedimento penale[243]. Il software integrato nei dispositivi di uso commerciale si limita ad autenticare l'individuo precedentemente registrato, in modalità 1:1. Generalmente, questi dispositivi, grazie alle tecniche di apprendimento automatico, sono in grado di eseguire le comparazioni fra i dati biometrici forniti a partire dalla registrazione della semplice immagine digitale, senza dover ricorrere all'ulteriore trasformazione della stessa in un modello elettronico o *template*[244]. In questo caso, ai fini dell'acquisizione di tale informazione entro il compendio probatorio, il canale di ingresso potrebbe essere individuato nell'art. 189 c.p.p., dal momento che la *ratio* della norma, come già accennato, consiste proprio nell'«evitare eccessive restrizioni ai fini dell'accertamento della verità, tenuto conto del continuo sviluppo tecnologico che estende le frontiere dell'investigazione, senza mettere in pericolo le garanzie difensive»[245]. Infatti, ciò che cambia in modo ineludibile è la natura del ricognitore che esegue la comparazione 1:1; in un caso "un programma", nell'altro l'"uomo". Peraltro, parte della dottrina ha già proposto una soluzione di tal genere, considerando il risultato della comparazione automaticamente generata come un prodotto atipico del riconoscimento fotografico autonomamente curato dalla polizia giudiziaria, a sua volta prodotto atipico dell'atto di indagine di cui all'art. 361 c.p.p.[246].

[243] Cfr. il capitolo III, § 1 e 1.3.

[244] Cfr. il capitolo I, § 2.2.

[245] Cfr. la *Relazione al progetto preliminare del codice di procedura penale*, p. 60, reperibile all'indirizzo https://www.gazzettaufficiale.it/eli/id/1988/10/24/088A4237/sg (visualizzato in data 21.7.2021).

[246] Cfr. G. Canzio, Intelligenza artificiale, algoritmi e giustizia penale, in *www.sistemapenale.it*, 8.1.2021, ove l'Autore considera più in generale l'*electronic evidence* scaturente da software di IA. Con riferimento ad un *match* generato da un software di

Da qui, la necessità di considerare innanzitutto il primo requisito richiesto dall'art. 189 c.p.p., ossia quello dell'idoneità accertativa del fatto che, come visto *supra*[247], viene valutato in base ai parametri individuati nel noto caso *Daubert*[248] della Corte Suprema degli Stati Uniti, risalente agli inizi degli anni Novanta e fatti propri con alcune modifiche dalla nostra giurisprudenza. A tal proposito, dunque, aldilà dell'impiego di SARI *Enterprise* da parte delle forze di polizia, il cui risultato non è mai oggetto diretto di valutazione da parte del giudice, forse varrebbe più la pena concentrarsi sul risultato di compatibilità generato automaticamente tra un volto precedentemente registrato e quello impiegato per accedere in un luogo fisico o in un sistema. Rispetto a questo tipo di dato può essere molto complesso risalire ai tassi di falsi positivi e falsi negativi e al procedimento eseguito per validare il sistema. Oltre a ciò, non è detto che dalla rappresentazione digitalizzata del dato ovvero dal suo modello elettronico registrato nel *repository* si riescano ad estrarre informazioni rilevanti per l'accertamento dei fatti oggetto del procedimento. Inoltre, il risultato di compatibilità o meno tra due volti, ottenuto da una comparazione eseguita da un dispositivo IoT, dev'essere effettivamente compreso dal giudice e si deve poter concretamente ricostruire e valutare l'attendibilità di tutti i singoli passaggi intermedi. E questo non è scontato che si verifichi. Invero, com'è stato evidenziato, «la nomina di un consulente tecnico per confutare la certificazione dell'*output* da parte della polizia scientifica può rivelarsi inefficace; in particolare, quando la corrispondenza tra i volti comparati sia espressa per grado di similarità, non risultando *ictu oculi* attendibile o inattendibile, il relativo risultato, frutto di una tecnologia automatizzata, rischia di "ammaliare" con le sue suggestioni l'operatore, probabilmente restio, magari anche inconsciamente, ad abbandonare l'ipotesi del software»[249].

Infine, anche qualora fosse accertabile e accertato «che l'attività automatizzata di ricognizione superi per affidabilità di risultati, quella tradizionalmente riservata alla capacità mnesica dell'uomo»[250], occorrerebbe comunque considerare il secondo requisito dettato dall'art. 189 c.p.p. concernente il rispetto della libertà morale. Per vero, con riferimento a tale parametro non

riconoscimento facciale, cfr. R. Lopez, *La rappresentazione facciale tramite software*, in AA.VV., *Le indagini atipiche*, (a cura di) A Scalfati, Giappichelli, Torino, 2019, p. 253.

[247] Cfr. il capitolo III, § 1.1.

[248] *Daubert v. Merrel Dow Pharmaceuticals Inc*., 509 U.S. 579 (1993).

[249] Cfr. R. Lopez, *La rappresentazione facciale tramite software*, cit., pp. 312 e ss. L'Autrice continua affermando che «(…) il limite del S.A.R.I., (…) così come di ogni altro programma di riconoscimento facciale da impiegare in ambito investigativo, sembra risiedere proprio in una ripetibilità solo apparente dell'atto identificativo. Infatti, per quanto l'operazione automatizzata risulti sempre replicabile, potendo la medesima immagine fotografica essere processata dal software un numero indefinito di volte senza pregiudizio per la sua integrità, la ripetizione del riconoscimento resta, comunque, di dominio esclusivo della "macchina" e dell'operatore che la interroga: l'attività che è *off limits* per la difesa, preclude ogni tentativo di falsificazione del relativo risultato in contraddittorio. Unico oggetto di confronto dialettico con l'accusa riguarderà soltanto la fonte mediata, ossia la relazione della polizia scientifica illustrativa della verifica di affidabilità dell'*output*, attraverso gli standard identificativi classici, fondati su parametri discriminatori sia metrici […], che fisionomici».

[250] Cfr. R. Lopez, *La rappresentazione facciale tramite software*, cit., p. 313.

sorgerebbero particolari criticità. Come già anticipato *supra*[251], per il momento è da escludersi un'intrusione della libertà morale dell'individuo, dal momento che i «dati biometrici eventualmente utilizzati per essere confrontati con quelli della persona indagata o sospettata sono acquisiti sulla base di una normativa *ad hoc*, che ne garantisce l'utilizzo trasparente e per fini legittimi»[252]. Tuttavia, l'impianto normativo attuale risulta ancora troppo frammentario e, in alcuni casi, troppo risalente per poter regolamentare ogni aspetto legato all'impiego sistematico di tali strumenti automatici. V'è da aggiungere che l'art. 189 c.p.p. risulta estremamente generico. Infatti, «dopo aver stabilito il limite della libertà morale e quello della idoneità all'accertamento dei fatti», la disposizione «lascia all'autorità procedente totale libertà nel determinare le modalità con le quali la prova atipica deve essere acquisita, salva la necessità del contraddittorio con le parti, preventivo, quando possibile, ovvero successivo in relazione agli atti a sorpresa»[253].

2.3.3. Il S.A.R.I. *Real time*: una proposta di inquadramento

Nonostante l'impiego della modalità applicativa "*Real time*" di S.A.R.I. risulti ad oggi controversa per le descritte motivazioni[254], si ritiene opportuno richiamare brevemente quanto già anticipato *supra*[255]. L'utilizzo di questa versione del software infatti potrebbe ragionevolmente accostarsi alla disciplina di matrice giurisprudenziale enunciata per le videoregistrazioni eseguite in spazi aperti al pubblico o in luoghi privati[256]. In particolare, si ritiene che la classificazione operata nella sentenza delle Sezioni unite "Prisco" sia da considerare un preliminare punto di partenza per l'introduzione di una disciplina che stabilisca i casi e i modi di impiego di questo inedito mezzo di ricerca della prova. In questo modo, l'individuo saprebbe come e per quale ragione la sua impronta facciale risulti captata e simultaneamente comparata e si potrebbe tutelare così «la stessa libertà morale della persona intesa come facoltà di autodeterminarsi rispetto agli stimoli»[257].

[251] Cfr. il capitolo III, § 2.1.2.
[252] Cfr. M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Diritto Penale e Processo*, n. 8/2021, p. 1054.
[253] Cfr. C. Conti, *Accertamento del fatto e inutilizzabilità nel processo penale*, Cedam, Padova, 2007, pp. 152 e ss.
[254] Cfr. il § 2.1.1.
[255] Cfr. il capitolo II, § 1.4.2.
[256] Si rimanda la trattazione al capitolo II, § 1.4.2.
[257] Cfr. M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, cit., p. 1054. Dello stesso avviso E. Currao, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, cit., p. 11.

3. Riconoscimento facciale e diritti fondamentali coinvolti

Una volta inquadrato più specificamente il funzionamento delle tecnologie di riconoscimento facciale, occorre stabilire quali siano i diritti e le libertà fondamentali su cui esse risultano potenzialmente in grado di incidere, e in quali modalità questo possa avvenire nel contesto di *law enforcement*. Trattasi di un'analisi che solo di recente è stata oggetto di attenzione in ambito europeo[258], nonostante la dottrina statunitense abbia già affrontato il tema da ormai più di un ventennio. Infatti, tra le particolarità che connotano le tecniche di riconoscimento facciale, oltre a quelle già descritte, vi è la capacità di influenzare e «condizionare contestualmente e trasversalmente»[259] molteplici diritti fondamentali.

Pur tenendo conto delle necessarie distinzioni in relazione all'impiego concreto del riconoscimento facciale, nei successivi paragrafi verrà eseguita l'analisi delle tecnologie di riconoscimento facciale automatiche nello spettro delle garanzie potenzialmente coinvolte, al fine di illustrare come tali intrusioni possano concretamente avvenire.

3.1. L'impiego dei dispositivi in "*real time*" e diritti fondamentali

In primo luogo, al fine di poter condurre un'analisi sui potenziali rischi di violazione di garanzie e diritti fondamentali, occorre tenere distinti gli ambiti e le modalità applicative del riconoscimento "in tempo reale" e "in differita"[260].

3.1.1. Il riconoscimento in "*real time*" e la libertà personale

Mentre il ricorso alle tecniche di riconoscimento facciale "in tempo reale" non solleverebbe particolari criticità con riferimento alla libertà personale, intesa - nella accezione più ristretta - come tutela da coercizioni fisiche[261], l'impiego delle stesse potrebbe implicare taluni rischi per la libertà personale dell'individuo, intesa nel suo significato più ampio di "libertà morale" o "dignità sociale"[262]. Infatti, come è stato già evidenziato[263], il criterio di riferimento sarebbe la "degradazione giuridica dell'individuo" che comporterebbe un «assoggettamento totale della persona all'altrui potere»[264]. In

[258] Cfr. FUNDAMENTAL RIGHTS AGENCY, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27.11.2019, pp. 4 e ss., reperibile all'indirizzo https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law (visualizzato in data 28.12.2021).
[259] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 58.
[260] Cfr. *supra* il § 1.3.
[261] Ovviamente fatto salvo il caso in cui il rifiuto alla sottoposizione al riconoscimento faccia scattare l'uso della forza.
[262] Cfr. il capitolo III, § 2.1.
[263] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 82.
[264] Cfr. C. Cost., n. 11/1956, reperibile in www.cortecostituzionale.it (visualizzato in data 28.12.2021).

tal senso, questa modalità applicativa potrebbe produrre una condizione e uno stato psicologico di "assoggettamento" conseguente ad un'attività di sorveglianza diretta nei confronti del singolo individuo, in ragione di una sua particolare condotta, ovvero della sua presenza in una determinata area geografica. Tale potere, come si approfondirà meglio *infra*[265], è in grado di influenzare il comportamento e le abitudini delle persone che, pur di sottrarsi a forme di controllo generalizzate, potrebbero preferire limitare anche le più elementari attività quotidiane.

La *quaestio* rimane aperta dal momento che le variabili in gioco sono diverse, tra le quali spiccano l'introduzione di sempre più innovative soluzioni tecnologiche e le molteplici potenzialità lesive dei diritti fondamentali. Rispetto alla libertà personale, intesa dunque nel suo significato più ampio, non è ancora possibile delimitare nettamente il confine con le altre libertà tutelate in Costituzione[266].

3.1.2. Il riconoscimento in "*real time*" e il diritto alla riservatezza

Particolare rilevanza assume poi, come visto[267], il "proteiforme" diritto alla *privacy* riconosciuto e tutelato dagli artt. 8 Conv. eur. dir. uomo, 7 e 8 CDFUE[268], «nonostante sia ancora diffusa l'idea che la natura pubblica del luogo in cui avviene la rilevazione determinerebbe un'implicita rinuncia alla riservatezza»[269]. V'è da sottolineare che il novero delle informazioni potenzialmente ricavabili tramite le tecnologie di riconoscimento facciale impiegate in tempo reale non coincide più con l'insieme di dati che rivelerebbe la semplice esposizione al pubblico[270]. Memori dei riferimenti normativi sulla protezione dei dati entro cui si colloca l'impiego di questa particolare tecnologia, l'analisi si concentrerà su un discusso caso di utilizzo del processo automatizzato di riconoscimento facciale da parte delle forze di polizia straniere per finalità di sicurezza, al fine di dimostrare quanto risulti ormai complesso il raggiungimento di un punto di equilibrio tra le esigenze di sicurezza e il mantenimento dell'ordine pubblico, da una parte, e le diverse libertà esercitabili fisicamente nella dimensione pubblica, dall'altra.

---

[265] Cfr. *infra* il § 3.1.5.

[266] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 84 ove l'Autore richiama a tal proposito l'art. 23 Cost. intendendo la sottoposizione ad un procedimento di identificazione tramite tecniche di riconoscimento facciale senza il proprio consenso come un "obbligo personale".

[267] Cfr. il capitolo I, § 1.1 e capitolo III, § 2.4.

[268] Cfr. il capitolo III, § 2.4.

[269] Cfr. C. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *www.lalegislazionepenale.it*, 11.12.2021, pp. 13 e ss.

[270] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., pp. 78 e ss.

3.1.3. Un noto caso di impiego del riconoscimento facciale a fini di sicurezza e prevenzione

Nonostante un «*case law is still virtually non-existent*»[271], si ritiene utile richiamare la giurisprudenza d'oltremanica che per la prima volta ha approfondito l'analisi degli strumenti di riconoscimento facciale automatico rispetto a determinate garanzie fondamentali per l'individuo[272]. Dapprima la *High Court of Justice of England and Wales*[273] e, successivamente in sede di impugnazione, la *Court of Appeal of England and Wales*[274] si sono pronunciate sulla possibilità di impiego del cd. "*Automated Facial Recognition Locate*"[275], uno strumento di riconoscimento facciale in "tempo reale" in dotazione alla *South Wales Police* nell'ambito della realizzazione di un progetto pilota per finalità di sicurezza[276]. Quest'ultimo, tra i diversi programmi intrapresi nel Regno Unito, è stato avviato in assenza di una disciplina legislativa di riferimento che regolamentasse specificamente

[271] Cfr. FUNDAMENTAL RIGHTS AGENCY, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., p. 4. Cfr. anche M. Zalnieriute, *Burning Bridges: the automated facial recognition technology and public space surveillance in the modern State*, in *Colum. Sci. & Tech. L. Rev*., Vol. 22, p. 288.

[272] Cfr. "*Liberty fights for facial recognition ban following court ruling*", 4.9.2019, reperibile all'indirizzo https://www.libertyhumanrights.org.uk/issue/liberty-fights-for-facial-recognition-ban-following-court-ruling/ (visualizzato in data 3.12.2021).

[273] Cfr. HIGH COURT OF JUSTICE, *Queen's Bench Division, Divisional Court*, 4 settembre 2019, Case No: CO/4085/2018, R (Bridges) v. CCSWP e SSHD (d'ora in avanti: [2019] EWHC 2341 (Admin)). Per un primo commento v. J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del Garante privacy d'Oltremanica)*, in *www.sistemapenale.it*, 28.3.2020, A. Pin, *Non esiste la "pallottola d'argento": l'Artificial Face Recognition al vaglio giudiziario per la prima volta*, in *DPCE Online*, v. 41, n. 4, 2020, I. Borshoff, *UK court backs police in facial recognition lawsuit*, 2019, https://www.politico.eu/article/uk-court-backs-police-in-facial-recognition-lawsuit/ (visualizzato in data 7.1.2022). E. Faletti, *Face detection: per la prima volta il riconoscimento al vaglio dei tribunali*, in *Il Quotidiano giuridico*, 29.10.2019.

[274] Cfr. COURT OF APPEAL, R (Bridges) v. CCSWP e SSHD (d'ora in avanti: [2020] EWCA Civ 1058). Per un primo commento v. M. Zalnieriute, *Burning Bridges: the automated facial recognition technology and public space surveillance in the modern State*, cit., pp. 284 e ss., G. K. Y. Chan, *Towards a calibrated trust-based approach to the use of facial recognition technology*, in *International Journal of Law and Information Technology*, 2021, 00, pp. 13 e ss. e B. Keenan, *Automatic Facial Recognition and the Intensification of Police Surveillance*, in *Modern Law Review*, 2021, 84(4), pp. 886–897. Cfr. anche "*Surveillance Camera Commissioner's statement: Court of Appeal judgment (R) Bridges v South Wales Police – Automated Facial Recognition*", reperibile all'indirizzo https://www.gov.uk/government/speeches/surveillance-camera-commissioners-statement-court-of-appeal-judgment-r-bridges-v-south-wales-police-automated-facial-recognition (visualizzato in data 7.1.2022), "*UK Court of Appeal Finds Automated Facial Recognition Technology Unlawful in Bridges v South Wales Police*", reperibile all'indirizzo https://www.huntonprivacyblog.com/2020/08/12/uk-court-of-appeal-finds-automated-facial-recognition-technology-unlawful-in-bridges-v-south-wales-police/ (visualizzato in data 7.1.2022).

[275] Da ora in avanti "*AFRL*".

[276] È bene ricordare che nel Regno Unito sono stati avviati diversi progetti pilota che coinvolgono sistemi di riconoscimento facciale impiegati da vari corpi di polizia per finalità di prevenzione e repressione della criminalità. V. in particolare *London Metropolitan Police*, alla *South Wales Police* e alla *Leicestershire Police* nel report "*Algorithm use in the criminal justice system*", reperibile all'indirizzo https://www.lawsociety.org.uk/topics/research/algorithm-use-in-the-criminal-justice-system-report (visualizzato in data 3.12.2021). Il progetto pilota oggetto delle due pronunce giurisprudenziali ha riguardato l'impiego di entrambe le modalità di riconoscimento facciale poc'anzi descritte (v. *supra* il § 1.3). La prima, nota come "*Automated Facial Recognition Identify*", consiste nell'analisi di un'immagine di un soggetto la cui identità è ignota, la quale viene comparata con quelle contenute in un database della South Wales Police. La seconda modalità è invece quella eseguita "in tempo reale" (cd. "*AFRL*").

tale attività di tracciamento[277]. Più nel dettaglio, il ricorrente nel caso di specie lamentava di essere stato sottoposto, in modo illegittimo e senza che fosse mai stato inserito nelle liste dei sospettati (cd. *watchlist*), al software di riconoscimento facciale in tempo reale, mentre si trovava nella città di Cardiff[278]. La *South Wales Police*, secondo le doglianze dell'interessato, avrebbe impiegato tale strumento in assenza di una disciplina normativa autorizzativa *ad hoc*: da ciò sarebbe dunque derivata la lesione del suo diritto alla riservatezza, tutelato dall'art. 8 Conv. eur. dir. uomo, la violazione della disciplina eurounitaria e interna in materia di protezione dei dati personali e, infine, l'inosservanza di alcune disposizioni dell'*Equality Act*[279], potendo la tecnologia in esame, secondo il ricorrente, concretizzare il rischio di generare *bias* cognitivi[280] discriminatori nei confronti di donne e minoranze etniche[281]. Peraltro, la sentenza affronta le argomentazioni del ricorrente tralasciando un paradosso iniziale. Non era noto né al ricorrente, né alla polizia, né alla Corte se costui fosse stato effettivamente ripreso dalla telecamera[282]. Infatti, in mancanza di *match*, il software era stato programmato per eliminare automaticamente i dati biometrici raccolti[283].

Orbene, la *High Court of Justice* rigettava tutte le censure con una motivazione piuttosto articolata. In primo luogo, la Corte ha ammesso che l'impiego del software da parte della polizia gallese avesse certamente determinato un'ingerenza nella vita privata del ricorrente, potenzialmente lesiva dell'art. 8 Conv. eur. dir. uomo[284], dal momento che il rilievo e l'estrazione del suo profilo facciale costituiscono un «*information of an "intrinsically private" character*»[285]. Tuttavia, tale ingerenza nella sfera privata è stata ritenuta legittima poiché il § 2 della citata disposizione prevede che le autorità pubbliche possano compiere siffatta intrusione nella vita privata dei singoli laddove tale attività sia prevista «dalla legge e costituisca una misura che, in una società democratica, [sia] necessaria alla

[277] Cfr. B. Keenan, *Automatic Facial Recognition and the Intensification of Police Surveillance*, in *Modern Law Review*, Vol. 84, 4, 27.2.2021 e J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, cit., p. 7.

[278] Cfr. [2019] EWHC 2341 (Admin), §§ 11 ss.

[279] Reperibile all'indirizzo https://www.gov.uk/guidance/equality-act-2010-guidance (visualizzato in data 6.1.2021).

[280] I *bias* sono errori cognitivi che i sistemi di intelligenza artificiale commettono sulla base degli esempi che sono stati forniti loro. Per un approfondimento dei concetti richiamati, si veda A. Turing, *Intelligenza meccanica*, Bollati Boringhieri, Torino, 1994.

[281] Cfr. [2019] EWHC 2341 (Admin), § 20. Uno dei rischi più rilevanti nell'impiego di software di riconoscimento facciale è proprio legato alla discriminazione di determinate categorie di individui. Per un approfondimento v. FUNDAMENTAL RIGHTS AGENCY, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27.11.2019, cit., p. 4 e EUROPEAN PARLIAMENTARY RESEARCH SERVICE**,** *Regulating facial recognition in the EU*, September 2021, pp. 13 e ss., reperibile all'indirizzo https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf (visualizzato in data 17.1.2022).

[282] Cfr. [2019] EWHC 2341 (Admin), § 16.

[283] Cfr. [2019] EWHC 2341 (Admin), § 16.

[284] Cfr. [2019] EWHC 2341 (Admin), § 62.

[285] Cfr. [2019] EWHC 2341 (Admin), § 57. Lo stesso approccio – prosegue la *High Court* – si riscontra anche nel *case-law* della Corte di Giustizia dell'Unione europea, la quale, nel caso *Schwarz*, ha posto in relazione l'acquisizione di *fingerprints and facial images* con il diritto al «rispetto della vita privata con riguardo al trattamento dei dati personali», che concerne «ogni informazione relativa ad una persona fisica identificata o identificabile». Corte Giust. UE, 17 ottobre 2013, *Schwarz*, Causa C-291/12, § 48.

sicurezza nazionale, 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». Più nel dettaglio, la Corte ha ritenuto in primo luogo che l'attività di raccolta e di conservazione dei dati biometrici facciali tramite algoritmi rientri tra i poteri generali attribuiti alle forze di polizia per prevenire e contrastare la criminalità[286]. Oltre a ciò, l'impiego di strumenti di *facial recognition* rientrerebbe comunque nell'ambito di applicazione delle previsioni comuni (interne ed eurounitarie) di tutela della privacy[287], alle quali vanno aggiunte altresì una serie di disposizioni aventi rango regolamentare in tema di videosorveglianza e di *local policies* già adottate dalla *South Wales Police*[288]. In tal senso, il combinarsi delle diverse disposizioni citate costituirebbe quel «*clear and sufficient legal framework governing whether, when and how AFR Locate may be used*»[289], in conformità a quanto stabilito dall'art. 8 § 2 Conv. eur. dir. uomo.

Inoltre, secondo la Corte, le tecnologie di riconoscimento facciale andrebbero tenute distinte dall'estrazione del profilo del Dna e dal rilievo delle impronte digitali per scopi di identificazione, dal momento che «*no physical entry, contact or force is necessary when using AFR Locate to obtain biometric data*»[290]. Pertanto, non essendoci alcuna ingerenza fisica diretta sugli individui, allo stesso modo di quanto accade per le videoriprese[291], non sarebbe necessario che le autorità di *law enforcement* siano dotate di «*new express statutory powers*» per potersi avvalere dei software di riconoscimento facciale in tempo reale[292].

Con riferimento alla seconda doglianza del ricorrente, concernente la violazione della disciplina generale in materia di tutela della riservatezza, la Corte ha osservato che il procedimento di riconoscimento è stato condotto al fine di perseguire lo scopo legittimo di prevenzione e contrasto della criminalità, in modo del tutto conforme alla normativa (interna ed eurounitaria) in materia di trattamento dei dati personali[293]. In particolare, le autorità di polizia avrebbero predisposto garanzie particolarmente elevate rispetto alla *data retention*[294], informando la popolazione «*about AFR and as*

[286] Cfr. [2019] EWHC 2341 (Admin), § 68.

[287] Cfr. [2019] EWHC 2341 (Admin), §§ 84 e ss. In particolare, il *Data Protection Act* del 2018 «(…) *embeds key safeguards which apply to all processing of all personal data – including the biometric data processed when AFR Locate is used*». (Cfr. il § 85).

[288] La Corte si riferisce al "*Surveillance Camera Code of Practice*" e ad altri tre provvedimenti di rango non legislativo, il *SWP's Standard Operating Procedure*, il *SWP's Deployment Reports* e il *SWP's Policy on Sensitive Processing* (v. i §§ 89 e 92).

[289] Cfr. [2019] EWHC 2341 (Admin), § 84.

[290] Cfr. [2019] EWHC 2341 (Admin), § 75.

[291] Cfr. [2019] EWHC 2341 (Admin), §§ 73 e 75, ove la Corte, riferendosi ai software di riconoscimento facciale, specifica che «*the method is no more intrusive than the use of CCTV in the streets*».

[292] Cfr. [2019] EWHC 2341 (Admin), § 78.

[293] Cfr. [2019] EWHC 2341 (Admin), §§ 122 e ss.; 133 e ss.; 139 e ss. e 144 e ss.

[294] Cfr. [2019] EWHC 2341 (Admin), §§ 37 e ss. ove la Corte specifica che «(…) *if no match (false or positive) is made – as in the overwhelming majority of cases – then AFR Locate does not retain the facial biometrics or image of persons whose faces are*

to its use at the event or in the area which they may be attending or present»[295]. Oltre a ciò, prima di procedere con l'attività di *facial recognition* mediante videoripresa, la polizia gallese avrebbe adottato il programma denominato "*Policy on Sensitive Processing for Law Enforcement Purposes*"[296] con il quale venivano spiegate le attività compiute per «*securing compliance with the data protection principles*»[297] e un "*Data Protection Impact Assessment*"[298] con il quale veniva chiarito l'esatto funzionamento del sistema "*AFR Locate*" e i rischi per la protezione dei dati personali.

Infine, quanto ai potenziali effetti discriminatori della tecnologia nei confronti di minoranze etniche e delle donne, la Corte ha ritenuto che nel caso di specie non vi fosse «*firm evidence that the software does produce results that suggest indirect discrimination*»[299]. La *South Wales Police* aveva peraltro adottato un ulteriore provvedimento, l'"*Equality Impact Assessment – Initial Assessment*"[300], con il quale erano stati calcolati i rischi di eventuali discriminazioni derivanti dall'uso del software *de quo*.

Questo provvedimento, unitamente ad una dichiarazione di un funzionario della Divisione Servizi digitali diffusa il 26 novembre 2018[301] nella quale venivano fornite informazioni sul tasso di false corrispondenze, hanno condotto la Corte a ritenere che la *South Wales Police* avesse agito legittimamente. Giova, peraltro, evidenziare che la decisione in esame ha suscitato diverse critiche da parte dell'Autorità Garante per la protezione dei dati personali UK, ossia l'*Information Commissioner's Office*[302]. In primo luogo, in diversi documenti[303], l'*ICO* ha sottolineato i rischi attualmente esistenti legati all'impiego in luoghi aperti al pubblico della tecnologia di *live facial recognition* da parte delle forze di polizia nel Regno Unito. In particolare, l'*ICO* ha affermato che tale software dovrebbe essere impiegato solamente in presenza di «*specific serious or violent crimes*»[304] e non anche per forme di reato bagatellari. Oltre a ciò, dovrebbe essere sempre necessario specificare le

---

scanned. They are immediately and automatically deleted. That data is not available to the system operator or any other police officer».

[295] Cfr. [2019] EWHC 2341 (Admin), § 39.

[296] Cfr. [2019] EWHC 2341 (Admin), § 139.

[297] Cfr. [2019] EWHC 2341 (Admin), § 138.

[298] Cfr. [2019] EWHC 2341 (Admin), §§ 147 e ss.

[299] Cfr. [2019] EWHC 2341 (Admin), § 153.

[300] Cfr. [2019] EWHC 2341 (Admin), § 158.

[301] Cfr. [2019] EWHC 2341 (Admin), § 154.

[302] Da qui in avanti "*ICO*".

[303] Cfr. INFORMATION COMMISSIONER'S OPINION, "*Live facial recognition technology – police forces need to slow down and justify its use*", reperibile all'indirizzo https://ico.org.uk/about-the-ico/news-and-events/blog-live-facial-recognition-technology-police-forces-need-to-slow-down-and-justify-its-use/ (visualizzato in data 10.1.2022); "*ICO investigation into how the police use facial recognition technology in public places*", reperibile all'indirizzo https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf (visualizzato in data 10.1.2022); INFORMATION COMMISSIONER'S OPINION, "*The use of live facial recognition technology by law enforcement in public places*", reperibile all'indirizzo https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf (visualizzato in data 10.1.2022).

[304] Cfr. INFORMATION COMMISSIONER'S OPINION, "*The use of live facial recognition technology by law enforcement in public places*", cit., p. 15. Negli stessi termini, cfr. anche EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), *Facial recognition technology*, cit., p. 34.

ragioni per le quali non è possibile ricorrere a mezzi investigativi alternativi e meno invasivi[305]. A tal proposito, secondo l'*ICO*, la polizia gallese nel caso in esame «*had not ensured that a fair balance between the strict necessity of the processing of sensitive data and the rights of individuals had been struck*»[306].

Invero, come è stato sottolineato[307], l'*ICO* ha colto l'occasione per invitare le autorità governative ad adottare «*a statutory binding code of practice to provide further safeguards that address the specific issues arising from the use of biometric technology such as LFR*»[308]. Pertanto, secondo il *Commissioner*, è tempo che le forze politiche predispongano una normativa di riferimento vincolante, volta a stabilire quando e per quali reati le autorità di *law enforcement* possano avvalersi dei software di riconoscimento facciale[309]. In questo modo, si raggiungerebbe «*a highly desiderable level of clarity and consistency*» che «*would also contribute to the degree of transparency necessary as the use of LFR expands*»[310] e si limiterebbero gli effetti negativi che tale tecnologia può produrre sull'individuo.

La pronuncia della *Queen's Bench Division* della *High Court of Justice* è stata successivamente impugnata innanzi alla *Civil Division* della *Court of Appeal* e riformata con sentenza dell'11 agosto del 2020. Giova anticipare come le valutazioni totalmente divergenti fornite dalle due Corti sulla medesima vicenda processuale confermino la possibilità di interpretazioni dissonanti dei principi giuridici in gioco, quando lo scenario appaia del tutto inesplorato. Orbene, entrambi i giudici sono risultati concordi nel ritenere che l'impiego del sistema *AFR Locate* interferisca con il diritto al rispetto

---

[305] Cfr. INFORMATION COMMISSIONER'S OPINION, "*The use of live facial recognition technology by law enforcement in public places*", cit., p. 15.

[306] Cfr. INFORMATION COMMISSIONER'S OPINION, "*The use of live facial recognition technology by law enforcement in public places*", cit., p. 15.

[307] Cfr. J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, cit., p. 240.

[308] Cfr. INFORMATION COMMISSIONER'S OPINION, "*The use of live facial recognition technology by law enforcement in public places*", cit., p. 21.

[309] Uno dei più importanti risultati raggiunti in seguito alle riflessioni proposte dall'*ICO* è stato l'aggiornamento del "*Surveillance Camera Code of Practice*", ove si è specificato che «*any use of facial recognition or other biometric characteristic recognition systems needs to be clearly justified and proportionate in meeting the stated purpose, and be suitably validated. It should always involve human intervention before decisions are taken that affect an individual adversely*». Oltre a ciò, si è previsto che «(…) *when using a surveillance camera system for live facial recognition (LFR) purposes to find people on a watchlist, chief police officers should: set out and publish (a) the categories of people to be included on a watchlist and (b) the criteria that will be used in determining when and where to deploy LFR, having regard to the need only to do so for a lawful policing purpose; ensure that any biometric data that does not produce an alert against someone on the watchlist by the LFR system is deleted instantaneously or near-instantaneously; have regard to the Public Sector Equality Duty, in particular taking account of any potential adverse impact that the LFR algorithm may have on members of protected groups; establish an authorisation process for LFR deployments and identify the criteria by which officers are empowered to issue LFR deployment authorisations*». Il testo normativo è reperibile all'indirizzo https://www.gov.uk/government/consultations/surveillance-camera-code-of-practice/draft-updated-surveillance-camera-code-of-practice-accessible-version (visualizzato in data 10.1.2022). Peraltro, giova ricordare che, all'inizio di febbraio 2020, è stata presentata una proposta di legge, attualmente ancora in discussione presso il Parlamento britannico, tesa a introdurre una moratoria sull'uso ai fini di *law enforcement* del *live facial recognition* e ad avviare un percorso di riforma per disciplinare normativamente tale tecnologia. Il testo normativo proposto è reperibile all'indirizzo https://bills.parliament.uk/bills/2610 (visualizzato in data 10.1.2022).

[310] Cfr. "*The use of live facial recognition technology by law enforcement in public places*", cit., p. 21.

della vita privata. Tuttavia, diversamente da quanto stabilito dalla *Divisional Court*, ferma nel considerare che *l'AFR Locate* rientri nei «*common law powers*» della polizia, la *Court of Appeal* ha mosso le sue argomentazioni sulla base di differenti presupposti[311]. In primo luogo, secondo i giudici di seconde cure, l'«*AFR is a novel technology*». Essa «*involves the capturing of the images and processing of digital information of a large number of members of the public, in circumstances in which it is accepted that the vast majority of them will be of no interest whatsoever to the police*». Inoltre, «*it is acknowledged by all concerned that this is "sensitive" personal data*». Infine, «*the data is processed in an automated way*». Ne consegue, pertanto, che la normativa attualmente esistente non sembra sufficientemente specifica per rispondere all'interrogativo su chi effettivamente possa essere inserito nelle *watchlists* e in quali luoghi tali sistemi possano essere collocati. Secondo la Corte, dunque, l'operatore di polizia, nell'impiegare incondizionatamente tale strumento sulla popolazione, agirebbe con un'eccessiva discrezionalità[312]. Peraltro, la *Civil Division* aggiunge che nella vicenda in esame non sarebbe stato rispettato nemmeno il requisito della "stretta necessità" del trattamento dei dati sensibili, come richiesto dall'art. 10 della direttiva 2016/680/UE[313], secondo il quale tale trattamento è autorizzato «solo se strettamente necessario» rispetto alle finalità da perseguire. La *Court of Appeal* ha riformato così la pronuncia della *High Court* stabilendo che la normativa vigente non possa essere considerata sufficiente rispetto a quanto richiesto dall'art. 8 § 2 Conv. eur. dir. uomo. A tal proposito, di particolare rilevanza sono state le considerazioni della Corte d'Appello in merito alla necessità dell'intervento di un magistrato nell'autorizzare l'uso dell'*AFR Locate*[314]. Per i giudici di seconde cure, infatti, l'inserimento nelle *watchlist*, senza l'autorizzazione di un magistrato, di persone per le quali si ritiene necessaria l'attività di *intelligence,* pare del tutto irragionevole. Ciò a maggior ragione se si considera che per l'inserimento nelle *watchlist* di persone sospettate o accusate di reati sia in ogni caso necessaria l'approvazione da parte di un giudice[315].

Un ulteriore motivo di doglianza da parte del ricorrente concerneva un altro aspetto della violazione del diritto al rispetto della vita privata tutelato dall'art. 8 Conv. eur. dir. uomo, ossia quello del test di "proporzionalità" nell'impiego dell'*AFR Locate* rispetto alle condizioni stabilite nel § 2 della citata disposizione. La *Court of Appeal*, in questo caso si è limitata a respingere le censure dei ricorrenti senza sovrapporre alcuna valutazione o dichiarare errata l'analisi della *Divisional Court*[316]. Forse la Corte avrebbe potuto argomentare maggiormente questo punto, non limitandosi ad asserire che

[311] Cfr. [2020] EWCA Civ. 1058 §§ 86 e ss.
[312] Cfr. M. Zalnieriute, *Burning Bridges: the automated facial recognition technology and public space surveillance in the modern State*, cit., p. 293.
[313] Cfr. il capitolo I, § 1.1.
[314] Cfr. [2020] EWCA Civ. 1058, § 126.
[315] Il riferimento è al *Regulation of Investigatory Powers Act* 2000.
[316] Cfr. [2020] EWCA Civ. 1058, §§ 132 e ss.

l'intrusione nei confronti dell'interessato è stata «*negligible*» e che «*an impact that has very little weight cannot become weightier simply because other people were also affected*»[317]. In altre parole, la Corte considera l'impiego di questo strumento di sorveglianza come in grado potenzialmente di produrre molteplici e distinti danni separati che colpiscono i singoli individui rispetto ad un danno aggregato che colpisce l'intera popolazione.

Da ultimo, con riferimento alla garanzia di evitare il più possibile il rischio di effetti discriminatori, la *Court of Appeal* ha affermato che le autorità pubbliche hanno il dovere di compiere tutti i passi che ragionevolmente si rendono necessari per prendere in considerazione l'impatto potenziale derivante dall'impiego di un nuovo strumento che potrebbe produrre effetti sproporzionati verso determinate categorie di persone. Si tratterebbe di un'obbligazione "di processo" e non "di risultato" che ha l'effetto di rendere responsabili i soggetti che ricorrono all'utilizzo di simili tecnologie[318]. L'attività di verifica del risultato scaturente dal software eseguita dall'operatore specializzato non è ritenuta dalla Corte di per sé sufficiente ad assolvere il citato obbligo delle autorità pubbliche, posto che «*human beings can also make mistakes*»[319]. Occorrerebbe, pertanto, secondo i giudici di seconde cure, conoscere l'esatta percentuale dei falsi positivi e dei falsi negativi tra donne e uomini, ma ciò risulta difficilmente praticabile, posto che i dati, se valutati incompatibili dal software, vengono eliminati istantaneamente o dopo poco tempo[320].

Particolarmente rilevanti risultano poi le considerazioni sull'assenza di controlli sul *dataset* utilizzato per "allenare" l'algoritmo. Ciò in ragione del fatto che vi siano «*reasons of commercial confidentiality*» che hanno impedito di fatto alle autorità di polizia di verificare se siano presenti o meno *bias*[321] inaccettabili che possano produrre discriminazioni[322]. Trattasi di un passaggio obbligatorio che grava sulle autorità pubbliche e che deve compiersi per poter utilizzare legittimamente una simile «*novel and controversial technology*»[323].

Per tutto quanto sopra esposto, la *Court of Appeal* ha stabilito pertanto che «*the Respondent's use of Live Automated Facial Recognition technology was not in accordance with the law for the purposes of Article 8(2), (…)did not comply with section 64(3)(b) and (c) of the Data Protection Act 2018 (…)*» e «*did not comply with the Public Sector Equality Duty in section 149 of the Equality Act 2010 (…)*»[324]. Per vero, da questa seconda pronuncia si deduce che, allo stato attuale, la copertura normativa per far

[317] Cfr. [2020] EWCA Civ. 1058, § 143.
[318] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 238.
[319] Cfr. [2020] EWCA Civ. 1058, § 185.
[320] Cfr. [2020] EWCA Civ. 1058, § 191.
[321] Cfr. nota n. 280.
[322] Cfr. [2020] EWCA Civ. 1058, § 199.
[323] Cfr. [2020] EWCA Civ. 1058, § 201.
[324] Cfr. [2020] EWCA Civ. 1058, § 210.

fronte all'impiego del riconoscimento facciale in "*real time*" risulta piuttosto scarna e per certi versi inadeguata. La *Court of Appeal*, tuttavia, invece di evidenziare l'urgenza di una riforma normativa su scala nazionale, ha invitato ciascun dipartimento di polizia a dotarsi di proprie linee guida per l'impiego di questa tecnologia. Questo potrebbe senz'altro portare ad un'ulteriore frammentazione nella regolamentazione in tutto il Regno Unito, generando ancora più confusione[325]. Si ritiene, infatti, che la Corte avrebbe piuttosto dovuto incoraggiare lo sviluppo di un quadro normativo completo, limitando in questo modo l'eccessiva discrezionalità in capo alle autorità di polizia e prevenendo i rischi di violazione dei diritti fondamentali dell'individuo.

Dal canto nostro, com'è stato evidenziato in dottrina, si può legittimamente dubitare del fatto che anche una disposizione come «l'art. 189 c.p.p. soddisfi i principi di legalità e proporzionalità cui deve sottostare ogni ingerenza nel diritto in questione»[326]. In altre parole, «*the "law" must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity*», specificando quali siano i luoghi da sottoporre a osservazione ("*where question*") e chi può rientrare nella *watchlist* ("*who question*") al fine di «*give the individual adequate protection against arbitrary interference*»[327]. Entro tale scenario, poste le già evidenziate analogie con la disciplina delle videoregistrazioni e la prefigurata possibilità di applicazione dell'art. 189 c.p.p. a ipotesi di utilizzo del riconoscimento facciale "in tempo reale" in spazi aperti al pubblico (cfr. *supra* il § 2.3.3), lo scarno telaio di tale disposizione non consentirebbe al singolo di «mantenere il controllo» rispetto agli ambiti della propria vita privata, dal momento che la norma «fissa soltanto i limiti esterni della idoneità all'accertamento dei fatti e del divieto di compromettere la libertà morale della persona, lasciando scoperti aspetti normativi essenziali del potere probatorio»[328]. Oltre a ciò, come specificato dalla *Court of Appeal*, le autorità di polizia non sembrano ancora in grado di verificare con esattezza il corretto funzionamento dei sistemi utilizzati, superando efficacemente le barriere opposte dal segreto, con rilevanti conseguenze sulla verifica dell'idoneità ad accertare i fatti dello strumento considerato.

È bene tenere in ogni caso in considerazione che la *South Wales Police* può continuare ad utilizzare questa modalità applicativa del riconoscimento facciale[329], per esempio, al fine di far fronte a

[325] In questo senso cfr. M. Zalnieriute, *Burning Bridges: the automated facial recognition technology and public space surveillance in the modern State*, cit., p. 303.

[326] Cfr. G. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato*, cit., p. 15.

[327] Cfr. [2020] EWCA Civ. 1058, §§ 91 e ss.

[328] Cfr. D. Negri, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Rivista Italiana di Diritto e Procedura Penale*, fasc.1, 1.3.2020, p. 3.

[329] Cfr. "*Faceoff! UK appellate court finds police use of facial recognition technology contravenes laws*", reperibile all'indirizzo https://www.torkinmanes.com/our-resources/publications-presentations/publication/faceoff-uk-appellate-court-finds-police-use-of-facial-recognition-technology-contravenes-laws (visualizzato in data 10.1.2022). Cfr. anche M. Zalnieriute, *Burning Bridges: the automated facial recognition technology and public space surveillance in the modern State*, cit., p. 297.

specifiche esigenze di indagine[330]. A tal proposito, il *Surveillance Camera Commissioner*[331] ha formulato alcuni principi per guidare un impiego virtuoso di tali strumenti da parte delle forze di polizia e al fine di porre rimedio a tale situazione di incertezza[332], ulteriormente esasperata dalle contrastanti pronunce in esame.

3.1.4. Il riconoscimento in "*real time*" e la libertà di espressione e manifestazione del pensiero

Tra i molteplici diritti fondamentali potenzialmente influenzati dall'impiego deregolamentato delle tecnologie di *live facial recognition* per scopi di prevenzione, indagine e contrasto al crimine, figura altresì la libertà di manifestazione del pensiero[333]. Essa è stata in primo luogo definita come un «elemento essenziale della vita di uno Stato democratico, secondo quella direttrice che ha trovato esplicitazione nella dimensione partecipativa di tutti i diritti costituzionali codificata nell'art. 3 c. 2, Cost.»[334]. A rilevare qui è la possibilità per l'individuo di esercitare liberamente il proprio diritto a contrapporsi alle forze governative nella discussione di problemi o nell'elaborazione collettiva di proposte politiche. In questo senso, i sistemi di riconoscimento facciale impiegati nel corso di manifestazioni pubbliche «possono divenire agilmente strumenti di repressione o, più in generale, di limitazione di tali eventi»[335]. I partecipanti, infatti, come attestano anche le indagini compiute dal Consiglio per i diritti umani delle Nazioni Unite[336], potrebbero sentirsi limitati nell'esercizio della libertà di manifestazione del pensiero, specialmente quando il sistema sia in grado di acquisire e

---

[330] A titolo esemplificativo v. "*Facial recognition: How South Wales Police caught a sexual predator*", reperibile all'indirizzo https://www.bbc.com/news/uk-wales-55842869 (visualizzato in data 10.1.2022); "*Police are using hand-held facial recognition cameras on the streets for the first time - allowing suspects to be identified on the spot even if they refuse to co-operate*", reperibile all'indirizzo https://www.dailymail.co.uk/news/article-10298385/Police-using-hand-held-facial-recognition-cameras-streets-time.html (visualizzato in data 10.1.2022).

[331] Trattasi dell'autorità indipendente istituita ai sensi del *Protection of Freedoms Act* del 2012 avente la funzione di esercitare un controllo sul rispetto del "*Surveillance Camera Code of Practice*". Cfr. https://www.gov.uk/government/organisations/surveillance-camera-commissioner/about (visualizzato in data 10.1.2022).

[332] "*Facing the Camera Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales*", reperibile all'indirizzo https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf (visualizzato in data 10.1.2022).

[333] Tale libertà è strettamente connessa alla libertà di riunione che sarà oggetto di approfondimento nel successivo § 3.1.5. Su questo punto v. in primo luogo EUROPEAN PARLIAMENTARY RESEARCH SERVICE**,** *Regulating facial recognition in the EU*, September 2021, pp. 8 e ss., reperibile all'indirizzo https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf (visualizzato in data 17.1.2022).

[334]Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 101.

[335]Cfr. E. Currao, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, cit., p. 13.

[336]Cfr. HUMAN RIGHTS COUNCIL - SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION, *Surveillance and human rights: report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, reperibile all'indirizzo https://digitallibrary.un.org/record/3814512#record-files-collapse-header (visualizzato in data 11.1.2022).

conservare tutte le immagini e non solo quelle riferite a soggetti già noti alle forze di polizia. Come sottolineato, «a risultarne svilita, così, è quella prospettiva "funzionalista" che nel nostro ordinamento ha legato questa libertà alle forme proprie di una democrazia pluralista, entro cui la possibilità di esprimere la propria opinione viene tutelata come valore in sé e non per i contenuti del messaggio espresso»[337].

Anche l'Agenzia UE per i diritti fondamentali[338] e l'*European Data Protection Supervisor*[339] hanno sollevato analoghe perplessità circa i potenziali rischi derivanti dall'impiego della tecnologia di *facial recognition*, specie se utilizzata in modalità *live*, in luoghi aperti al pubblico e in occasione di eventi o manifestazioni, potendo le persone sottoposte a mezzi di sorveglianza di massa «*change their behaviour, withdrawing from social life, not visiting central places under surveillance, avoiding train stations or declining to attend cultural, social or sports events*»[340]. A tal proposito, si definisce "*chilling effect*" lo stato di «soggezione e di timore»[341] dei cittadini posti di fronte alla prospettiva di essere sottoposti al riconoscimento facciale per l'attraversamento di una determinata area geografica[342]. Come è stato peraltro evidenziato dalla dottrina, «l'impiego degli strumenti di riconoscimento facciale *real time* (…) ha finito per offrire un'argomentazione in più a quanti sostengono da tempo che le tecnologie di videosorveglianza in generale e, data la loro maggiore intrusività, quelle di identificazione biometrica basate sui tratti caratteristici del volto in particolare possono determinare nei consociati un atteggiamento di auto-censura (…)»[343].

Per tale ragione, secondo l'Agenzia UE per i diritti fondamentali, posto che l'impiego di tali strumenti potrebbe determinare una rilevante compressione di questa libertà, è necessario compiere un «*strict necessity and proportionality test, including a clear legal basis to do so and a legitimate*

---

[337]Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., pp. 102 e 103.

[338]Cfr. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27.11.2019, pp. 29 e ss., reperibile all'indirizzo https://fra.europa.eu/en/publication/2019/facial-recognition (visualizzato in data 11.1.2022).

[339] Cfr. *"Facial recognition: A solution in search of a problem?",* reperibile all'indirizzo https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en (visualizzato in data 11.1.2022).

[340] Cfr. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., p. 20.

[341] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 59.

[342] Cfr. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., p. 30, ove peraltro specifica che «*this chilling effect also has clear implications vis-à-vis the effective functioning of participatory democracy, and thus directly interferes with the freedom of assembly and association*». Su questo punto v. anche F. Paolucci, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, In *Medialaws*, 1/2021, p. 214, M. Zalnieriute, *Burning Bridges: the automated facial recognition technology and public space surveillance in the modern State*, cit., p. 299, EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Person identification, human rights and ethical principles. Rethinking biometrics in the era of artificial intelligence*, 2021, p. 33, reperibile all'indirizzo https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)697191 (visualizzato in data 2.2.2022) e E. Selinger, B. Leong, *The Ethics of Facial Recognition Technology*, in AA.VV., *The Oxford Handbook of Digital Ethics*, (a cura di) C. Veliz, Oxford, 2021, p. 11.

[343]Cfr. C. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato*, cit., p. 12.

aim pursued»[344]. Occorre regolamentare, se non limitare, quell'«erosione generalizzata dell'anonimità in pubblico»[345], favorita dalla diffusione di forme di sorveglianza, praticate sia da autorità pubbliche sia da imprese private, verso la quale le tecnologie basate sul riconoscimento facciale si stanno irrimediabilmente orientando.

3.1.5. Il riconoscimento in "*real time*" e la libertà di riunione

Giova altresì fare cenno alla libertà di riunione, strettamente connessa alla libertà di manifestazione del pensiero, in relazione all'impiego di sistemi di riconoscimento facciale in modalità "*real time*"[346]. Per vero, l'ordinamento italiano, per l'esercizio di questa libertà, richiede il rispetto di alcuni requisiti oggettivi legati a talune particolari modalità di partecipazione. Basti ricordare il divieto di indossare «caschi protettivi», ovvero, «qualunque altro mezzo atto a rendere difficoltoso il riconoscimento della persona, in luogo pubblico o aperto al pubblico, senza giustificato motivo»[347]. A tal proposito, il Testo Unico delle Leggi di Pubblica Sicurezza (cd. TULPS)[348] fissa un generale divieto di «comparire mascherato in luogo pubblico»[349]. Analogamente a quanto previsto per l'esercizio della libertà di manifestazione del pensiero, posta la sottoposizione a riconoscimento facciale in un determinato luogo pubblico, «i partecipanti potrebbero decidere di rinunciare alla propria (…) libertà di riunione per evitare di essere inserit[i] – ingiustificatamente – all'interno di un archivio a disposizione delle forze dell'ordine»[350].

Si ribadisce l'insorgere della necessità di una complessa attività di bilanciamento che tenga conto di interessi opposti fondamentali e che deve essere eseguita caso per caso dall'interprete, ma che non può più prescindere da un intervento del legislatore.

---

[344]Cfr. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., p. 24.

[345] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 104. Su questo punto v. anche M. Zalnieriute, *Burning Bridges: the automated facial recognition technology and public space surveillance in the modern State*, cit., p. 299.

[346] V. anche in questo caso EUROPEAN PARLIAMENTARY RESEARCH SERVICE**,** *Regulating facial recognition in the EU*, September 2021, cit., pp. 13 e ss.

[347] Cfr. l'art. 5 della l. 22.5.1975, n. 152.

[348] Cfr. il Testo Unico delle leggi di pubblica sicurezza (da qui in avanti TULPS) – Regio decreto, 18 giugno 1931, n. 773.

[349] Cfr. l'art. 85 TULPS.

[350] Cfr. E. Currao, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, cit., p. 13. G. Di Paolo, *"Tecnologie del controllo" e prova penale*, cit., p. 286, con riferimento a strumenti di monitoraggio elettronico eseguito in ambiti pubblici ha affermato che «un controllo sistematico sugli spostamenti e sulle attività che le persone espletano in spazi pubblici, aperti o esposti al pubblico vada a minare indirettamente non soltanto la libertà di circolazione, ma anche, per esempio, la libertà di riunione».

3.1.6. Il riconoscimento in "*real time*" e il diritto all'autodeterminazione informativa

L'oggetto ultimo di tutela sembra allora essere rappresentato dalla libertà di autodeterminazione dell'individuo, intesa come «la radice di ogni libertà e la precondizione essenziale per la realizzazione di una società aperta e democratica»[351]. Più specificamente, tale diritto si sostanzia nella libertà di *autodeterminazione informativa* come garanzia prodromica all'esercizio di ulteriori libertà e al godimento di altri diritti fondamentali[352]. Essa è stata definita, da una parte, come «potere di esigere la rappresentazione integrale della identità "frammentata" e "decontestualizzata", tramite l'integrazione o la modifica dei propri dati» e, dall'altra, come potere di «revoca del consenso reso esplicitamente al trattamento» ovvero «limitazione del trattamento» e «cancellazione dei dati»[353]. Per vero, il presupposto logico per l'esercizio di tale libertà è costituito dal *diritto a ricevere conferma della sottoposizione ad un trattamento* specifico[354], dal quale peraltro si innescherebbe altresì il diritto ad accedere ai propri dati personali oggetto di trattamento[355]. A tal proposito, per quel che concerne specificamente le tecnologie di riconoscimento facciale questo diritto può essere esercitato anche in seguito alla captazione di un'immagine o di una videoripresa, ovvero nel momento in cui l'interessato ne ha appreso la notizia[356]. Peraltro, *condicio sine qua non* per l'esercizio di tale diritto è che il trattamento dei dati sia in ogni caso in corso, oppure vi sia conferma del fatto che vi sia la

[351] Cfr. G. Di Paolo, *"Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione*, Cedam, Padova, 2008, p. 153.

[352] Per un approfondimento cfr. S. Allegrezza, *Giustizia penale e diritto all'autodeterminazione dei dati*, in AA.VV., *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, (a cura di) D. Negri, Aracne, Roma, 2007, 2007, pp. 59 e ss.

[353] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., pp. 189 e 190. S. Carnevale, *Autodeterminazione informativa e processo penale*, in AA.VV., *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, (a cura di) D. Negri, Aracne, Roma, 2007, p. 7 la definisce come «la potestà del singolo sui dati a lui riferibili». S. Allegrezza, *Giustizia penale e diritto all'autodeterminazione dei dati*, cit., p. 60 definisce l'autodeterminazione informativa come un «diritto *in progress* (…) tanto è legato all'evoluzione delle tecnologie dell'informazione».

[354] Cfr. l'art. 14 della direttiva LED che dispone che l'interessato ha «il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: a) le finalità e la base giuridica del trattamento; b) le categorie di dati personali trattati; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano; f) il diritto di proporre reclamo all'autorità di controllo e le coordinate di contatto di detta autorità; g) la comunicazione dei dati personali oggetto del trattamento e di tutte le informazioni disponibili sulla loro origine». Analogamente dispone l'art. 15 del regolamento (UE) 2016/679 (GDPR).

[355] In questo senso v. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., p. 190.

[356] In particolare, il GRUPPO DI LAVORO - ARTICOLO 29, *Linee guida sul processo decisionale automatizzato relative alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, p. 30, dispone che «il titolare del trattamento deve fornire all'interessato informazioni sulle *conseguenze previste* del trattamento, piuttosto che una spiegazione di una *particolare* decisione».

conservazione dei *templates* biometrici ovvero della rappresentazione digitale dei dati[357]. E' chiaro che il diritto di accesso può trovare un contemperamento con l'esigenza di garantire la sicurezza pubblica e la repressione dei reati. Per tale ragione la direttiva 2016/680/UE (cd. LED) ha introdotto il regime di cd. "nessuna conferma, nessuna smentita"[358], che permette ai singoli Stati di limitare tale diritto all'informazione. In questo modo, l'interessato è posto nella condizione di esercitare comunque il suo diritto di accesso, ovvero richiedere spiegazioni tramite l'autorità di controllo qualora fossero previste tali forme di limitazione (cd. accesso indiretto)[359].

3.2. L'impiego dei dispositivi in "*post remote*" e i diritti fondamentali coinvolti

Si ritiene utile a questo punto della trattazione concentrarsi brevemente anche sull'analisi di quelle garanzie processuali fondamentali rispetto alle quali l'impatto del trattamento automatizzato dei dati, tramite un software impiegato in modalità *post remote*[360], rischia potenzialmente di porsi in contrapposizione. Si riprenderanno, pertanto, alcune riflessioni già anticipate *supra*, formulate con riferimento alla generalità delle tecniche automatiche di riconoscimento biometrico[361], calandole nel più specifico contesto dei software di *facial recognition* impiegati in modalità "a posteriori".

3.2.1. Il riconoscimento in "*post remote*", equo processo penale e parità delle armi

Volendo brevemente riprendere le considerazioni anticipate *supra* rispetto alla generalità degli *automated biometric recognition systems* nella prospettiva del "giusto processo" e del diritto di difesa[362], si ritiene opportuno formulare ulteriori riflessioni di dettaglio nella prospettiva dell'impiego più specifico di software di riconoscimento facciale. Si è già, peraltro, fatto cenno in precedenza all'impianto normativo di riferimento e alle interpretazioni giurisprudenziali più rilevanti ai fini della presente ricerca[363]. Tale prospettiva interessa parimenti i software impiegati in modalità "*real time*" e in "*post remote*"[364]. Ciò in ragione del fatto che in entrambi i casi l'impiego di un risultato di compatibilità scaturente fra due rappresentazioni digitalizzate di volti a fini investigativi o probatori

[357] Cfr. EUROPEAN DATA PROTECTION BOARD, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, 29.1.2020, p. 24.
[358] Cfr. GRUPPO DI LAVORO - ARTICOLO 29, *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, 29.11.2017, p. 21.
[359] Cfr. art. 17 LED.
[360] Cfr. *supra* il § 1.3.
[361] Cfr. il capitolo III, §§ 2 e ss.
[362] Cui si fa integralmente richiamo, cfr. il capitolo III, § 2.2.
[363] Cfr. il capitolo III, § 2.2.
[364] Cfr. *supra* per la distinzione fra le due modalità applicative il § 1.2.

potrebbe generare un potenziale attrito con gli artt. 6 § 3 Conv. eur. dir. uomo e 111 Cost. Infatti, come già emerso *supra*[365], si potrebbero verificare situazioni in cui emerga un effettivo sbilanciamento tra le parti, rispetto alla generale facoltà di introduzione di saperi specialistici nel procedimento.

Con specifico riferimento agli *automated facial recognition systems*, i potenziali profili di squilibrio conoscitivo che potrebbero manifestarsi tra le parti nel processo risultano essenzialmente due. In primo luogo, alcune problematiche potrebbero sorgere rispetto al dato biometrico digitale generato automaticamente da strumenti di uso generico o commerciale, quali assistenti domestici o dispositivi elettronici di rilevamento delle caratteristiche fisiologiche o comportamentali. In questo caso, infatti, oggetto di falsificazione delle parti non è il *match* o *non-match* scaturente fra due dati, successivamente verificato dall'intervento di un operatore, ma un confronto 1:1 eseguito automaticamente dagli algoritmi di un software, il cui funzionamento, sfuggendo ad un'effettiva comprensione, potrebbe determinare un rischio implicito per la parità delle armi. I software installati in *smartphone* o in dispositivi aventi un utilizzo generico o commerciale, peraltro, sono basati su tecniche computazionali che potrebbero vanificare la possibilità per le parti di verificare o falsificare un risultato di compatibilità prodotto automaticamente dagli stessi[366]. In attesa di analizzare e commentare le prime pronunce giurisprudenziali in materia, l'unica via per non disperdere queste informazioni potenzialmente decisive per le indagini e i processi penali sembra essere quella di una sistematica verifica della metodologia certificata e applicata in conformità ad una comune "*biometric chain of custody*"[367].

Con riferimento, invece, all'impiego del software di riconoscimento facciale applicato ad un'immagine sottoposta ad un procedimento di digitalizzazione ovvero ricavata da un *frame* di un video o da un'immagine digitale[368], si è osservato come, non potendo il *tool* restituire risultati certamente affidabili dal punto di vista forense[369], non sussisterebbero particolari problematiche con riferimento al rispetto del principio di parità delle armi, in ragione del fatto che il risultato di compatibilità generato è sottoposto alla verifica manuale da parte di un operatore specializzato. Ciò costituisce «una salvaguardia di importanza fondamentale per i diritti dei singoli»[370]: l'intervento

[365] Cfr. il capitolo III, § 2.2.

[366] Cfr. il capitolo III, § 2.2.

[367] Cfr. il capitolo II, § 1.3. V. su questo punto S. Quattrocolo, C. Anglano, M. Canonico, M. Guazzone, *Technical Solutions for Legal Challenges: Equality of Arms in Criminal Proceedings*, cit., p. 17, ove si afferma che «*independent review of data generated by automated process may grant validation of evidence*».

[368] Cfr. il capitolo II, § 1.

[369] Il software automatico, impiegato in fase investigativa, restituisce un risultato solamente "parziale", in quanto privo del calcolo del cd. "rapporto di verosimiglianza", oggetto di una successiva stima e valutazione da parte di operatori esperti (cfr. il capitolo I, § 3.3.1).

[370] Cfr. J. Della Torre, *Novità dal regno unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del garante privacy d'oltremanica)*, in *www.sistemapenale.it*, 28.3.2020, p. 235.

umano è, infatti, una garanzia importante, in grado di ridurre (ma non di eliminare) la probabilità che un soggetto subisca un errore valutativo da parte dell'algoritmo[371].

In secondo luogo, un potenziale profilo di disparità tra le parti nel procedimento potrebbe essere ragionevolmente individuato nel disporre di strumenti all'avanguardia in grado di estrapolare, analizzare e comparare automaticamente dei volti, dal momento che, come noto, «una delle parti – per lo più quella pubblica – ha accesso alla scienza e alle tecnologie migliori, disponendo di mezzi economici non limitati»[372]. A maggior ragione, come è stato evidenziato, «la prova algoritmica (…) introduce la forma più estrema di tale squilibrio, poiché il risultato probatorio può essere non criticabile laddove, appunto, l'inaccessibilità (…) [del] software non consenta alla parte contro la quale la prova è introdotta nel processo di contestarne l'accuratezza e l'attendibilità»[373]. A tal proposito, non si può fare a meno di accennare a una delle rare pronunce della Corte di cassazione che, seppur incidentalmente, ha trattato la questione[374]. Nel rigettare le doglianze difensive con le quali si contestava il mancato accoglimento da parte della Corte territoriale della richiesta di rinnovazione dell'istruttoria dibattimentale al fine di «procedere al riconoscimento facciale dell'imputato tramite la moderna tecnica S.A.R.I.», la Cassazione ha sottolineato quasi provocatoriamente come «la difesa non avesse in alcun modo documentato la valenza scientifica dell'anzidetta tecnologia». Quanto motivato così perentoriamente dalla Corte di cassazione rispetto alla semplice richiesta di impiegare tale software, e magari portare ulteriori elementi conoscitivi per la difesa nel procedimento, suona dunque piuttosto paradossale. Occorre, allora, non solo riflettere sulle effettive possibilità da parte della difesa di accedere, servirsi, dimostrare ed eventualmente falsificare tali strumenti a disposizione degli organi inquirenti, ma anche verificare se esistano ulteriori meccanismi, tecnici o processuali, che consentano alla difesa di esercitare fondatamente il proprio inviolabile diritto a criticare l'accuratezza della prova.

---

[371] Cfr. il capitolo II, § 2.1.

[372] Cfr. S. Quattrocolo, *Equita' del processo penale e automated evidence alla luce della convenzione europea dei diritti dell'uomo*, in *Revista Ítalo-Española de Derecho Procesal*, Vol. 1, 2019, p. 118.

[373] Cfr. S. Quattrocolo, *Equita' del processo penale e automated evidence alla luce della convenzione europea dei diritti dell'uomo*, cit., p. 118.

[374] Cfr. Cass. pen., Sez. IV, 18.6.2019, n. 39731, *inedita*. Si trova un cenno sulla pronuncia del 2019 anche in C. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato*, cit., p. 7. Un'ulteriore pronuncia ove si fa cenno a S.A.R.I. è Cass. pen., Sez. I, 21.7.2020, n. 21823, *inedita*, in cui la Corte sottolinea il valore meramente indiziario del risultato di compatibilità restituito dal software evidenziando come in quel caso «le immagini poste a base del riconoscimento non erano nitide e non consentivano di riconoscere le fattezze, l'abbigliamento e diversi particolari dell'accoltellatore, per cui non era sostenibile la sussistenza di elementi gravi».

3.2.2. Il riconoscimento in "*post remote*" e il principio del *nemo tenetur se detegere*

Come già anticipato[375], sono ormai piuttosto frequenti i casi in cui le autorità di polizia giudiziaria, al fine di accedere a determinati contenuti conservati all'interno di dispositivi digitali, sfruttano modalità applicative di sblocco del dispositivo tramite il riconoscimento biometrico con comparazione 1:1[376]. A tal proposito, si è menzionata una pronuncia della Corte europea dei diritti dell'uomo ove è stato cristallizzato il principio secondo il quale l'acquisizione di «*material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect*» si deve ritenere compatibile con il principio di *nemo tenetur se detegere* in quanto i mezzi intrusivi adottati avrebbero ad oggetto materiale estraneo all'area protetta dal diritto al silenzio[377]. In un'altra pronuncia, poi, la Corte ha sottolineato che, oltre alle caratteristiche del materiale oggetto di indagine, è necessario tenere in considerazione anche «*the nature and degree of the compulsion, the existence of any relevant safeguards in the procedures and the use to which any material so obtained is put*»[378]. Ciò posto, si ricorda che la Corte suprema olandese, in occasione di una recente pronuncia sul tema, ha stabilito che un'impronta digitale esista indipendentemente dalla volontà dell'indagato, e che il suo ottenimento non richieda, quindi, la collaborazione attiva dello stesso[379]. Pertanto, secondo l'*Hoge Raad*, l'atto coercitivo di apporre fisicamente il pollice dell'indagato sul sensore dello *smartphone*, al fine di sbloccare biometricamente il dispositivo, pur comportando una lieve costrizione della volontà del sospettato, non sarebbe in violazione del principio di *nemo tenetur se detegere*. Orbene, le conclusioni della Corte suprema olandese non possono essere ritenute condivisibili nel contesto tecnologico attuale. A maggior ragione se si considerano sistemi di riconoscimento come quello oggetto di analisi nel presente capitolo. L'atto di "carpire" l'immagine del volto al fine di accedere al contenuto conservato in un dispositivo digitale, senza che l'indagato ponga in essere un comportamento attivo nello svolgimento di tale attività o, addirittura, quest'ultima sia eseguita contro la sua volontà, costituisce una vera e propria forma di collaborazione nel

[375] Cfr. il capitolo III, § 2.2.1.

[376] Sul punto v. https://www.lastampa.it/tecnologia/news/2019/01/16/news/la-polizia-non-puo-costringere-a-sbloccare-un-iphone-protetto-da-faceid-o-touchid-1.33671588 (visualizzato in data 6.10.2021); https://www.forbes.com/sites/thomasbrewster/2016/10/16/doj-demands-mass-fingerprint-seizure-to-open-iphones/ (visualizzato in data 6.10.2021); https://appleinsider.com/articles/16/05/02/los-angeles-court-orders-woman-to-unlock-touch-id-equipped-iphone-for-fbi (visualizzato in data 6.10.2021); https://thenextweb.com/news/fbi-uses-faceid-to-unlock-a-suspects-iphone-x-for-the-first-time (visualizzato in data 6.10.2021); https://www.fairtrials.org/news/suspects-privilege-against-self-incrimination-not-violated-when-made-unlock-smartphone (visualizzato in data 6.10.2021).

[377] Cfr. *Saunders v. The United Kingdom*, cit., § 69.

[378] Cfr. *ex multis*, C. Edu, *Tirado Ortiz e Lozano Martin c. Spagna*, 15.6.1999; *Jalloh c. Germania*, 11.7.2006.

[379] Cfr. Hoge Raad, 9.2.2021, n. 19/05471, reperibile all'indirizzo https://linkeddata.overheid.nl/front/portal/document-viewer?ext-id=ECLI:NL:HR:2021:202 (visualizzato in data 6.10.2021).

procedimento che ragionevolmente deve essere ricondotta nella garanzia in esame[380]. E' tempo, pertanto, di rimeditare i confini delle tradizionali garanzie processuali, alla luce delle plurime peculiarità che caratterizzano i diversi strumenti di riconoscimento biometrico, in grado senza di dubbio di collezionare informazioni potenzialmente rilevanti per l'accertamento penale.

3.2.3. Il trattamento del dato biometrico digitalizzato nel rispetto del diritto alla riservatezza

Giova a questo punto proporre alcune brevi riflessioni rispetto al diritto alla riservatezza, architrave delle garanzie costituzionali contro le interferenze statuali, anche investigative[381], e al suo significato autentico, a fronte dell'impiego di strumenti automatici di riconoscimento facciale in modalità "*post remote*" da parte delle autorità di *law enforcement*. Anche l'Agenzia UE per i diritti fondamentali ha di recente sottolineato come «*the rights to respect for private life and data protection are central to the deployment of facial recognition technology*»[382]. Per entrambe le modalità applicative dei sistemi di riconoscimento facciale, infatti, tenendo conto della loro capacità di «*collecting, comparing and/or storing facial images in an IT system for identification purposes*», è ravvisabile «*an interference with the right to protection of personal data set out in Article 8 of the Charter (embodying pre-existing EU data protection law) and the right to private life under Article 7 of the Charter and Article 8 of the ECHR*»[383]. Oltre a ciò, i sistemi di riconoscimento facciale, posto che consentono l'estrazione «*of unique information and identifiers about an individual allowing his or her identification with precision in a wide range of circumstances*»[384], sono in grado di trattare informazioni dotate di un «*"intrinsically private" character*» che non viene meno in ragione del fatto che, per esempio, «*the biometric data is derived from a person's facial features that are "manifest in public"*»[385].

Considerata la complessa eterogeneità di provenienza delle rappresentazioni digitalizzate dei volti su cui è possibile eseguire una verifica automatica di compatibilità tramite software, occorre sempre valutare caso per caso l'eventuale grado di ingerenza nel diritto in esame. A tal proposito, come già

[380] In questo senso cfr. J. Czerniawski, C. Boyack, Reviewing the Privacy Implications of Law Enforcement Access to and Use of Digital Data, in *5 UTAH J. CRIM. L.* 73 (2021).
[381] Cfr. il capitolo III, § 2.4.
[382] Cfr. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27.11.2019, p. 23, reperibile all'indirizzo https://fra.europa.eu/en/publication/2019/facial-recognition (visualizzato in data 17.1.2022). Cfr. anche FUNDAMENTAL RIGHTS AGENCY, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27.11.2019, cit., p. 4 e EUROPEAN PARLIAMENTARY RESEARCH SERVICE**,** *Regulating facial recognition in the EU*, September 2021, p. 10 ove afferma che «*FRT implies the processing of data for the purpose of identification, it constitutes an interference with the right to data protection, as set out in Article 8 CFR and the right to private life under Article 7 CFR*».
[383] Cfr. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., p. 23.
[384] Cfr. HIGH COURT OF JUSTICE*, Queen's Bench Division, Divisional Court*, [2019] EWHC 2341 (Admin), § 57.
[385] Cfr. [2019] EWHC 2341 (Admin), § 57.

anticipato *supra*[386], l'art. 8 Conv. eur. dir. uomo tollera eventuali attentati alla vita privata degli individui, per far fronte a esigenze di giustizia, solo se «tale ingerenza sia prevista dalla legge» e sia «necessaria in una società democratica». Orbene, con riferimento all'impiego di un software di riconoscimento facciale in modalità "*post remote"* vale la considerazione già espressa *supra*[387], per cui - nel calibrare il rapporto tra il rispetto delle esigenze di accertamento dei fatti di reato e il sacrificio che può derivare ai diritti dei cittadini e alla loro riservatezza - sarebbe opportuno potenziare il coordinamento fra le disposizioni normative contenute nel "pacchetto di protezione dei dati" e le previsioni del codice di procedura penale, introducendo una regolamentazione più specifica e puntuale in materia di "*biometric chain of custody*"[388]. Infatti, si concorda con parte della dottrina che sostiene che «*national criminal procedural law would detail the conditions under which personal data can be requested, accessed and further used*»[389]. A maggior ragione, per quel che riguarda i risultati scaturenti da una comparazione di volti eseguita in modalità 1:1 tramite dispositivi IoT, ricondotti *supra*[390], in qualità di *automated electronic evidence*, nell'alveo dell'art. 189 c.p.p., si può legittimamente dubitare che la disposizione di riferimento possa concretamente soddisfare i principi di legalità e proporzionalità cui deve sottostare ogni ingerenza nel diritto in questione[391]. A tal proposito, si concorda con le parole utilizzate dalla *Civil Division* della *Court of Appeal* inglese, richiamata poc'anzi[392], che, riferendosi ai sistemi di riconoscimento facciale *real time* impiegati in luoghi pubblici da parte delle autorità del *South Wales Police*, ha affermato che «*the "law" must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity*», al fine di «*to give the individual adequate protection against arbitrary interference*»[393]. Quanto stabilito dall'art. 189 c.p.p. non può ad oggi essere considerato sufficiente per garantire al singolo la legittima aspettativa di mantenere il controllo sugli «ambiti di sviluppo della [propria] vita privata», dal momento che la disposizione fissa soltanto «i limiti esterni della idoneità all'accertamento dei fatti e del divieto di compromettere la libertà morale della persona, lasciando scoperti aspetti normativi essenziali del potere probatorio»[394].

[386] Cfr. il capitolo III, § 2.4.
[387] Cfr. il capitolo III, § 2.4.
[388] Cfr. il capitolo I, § 1.2.
[389] Cfr. C. Jasserand, *Reprocessing of biometric data for law enforcement purposes*, reperibile all'indirizzo https://pure.rug.nl/ws/portalfiles/portal/90355213/Complete_thesis.pdf (visualizzato in data 15.10.2021).
[390] Cfr. il capitolo III, § 1.3.
[391] Cfr. C. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato*, cit., p. 13.
[392] Cfr. *supra* il § 3.1.3.
[393] Cfr. [2020] EWCA Civ. 1058, §§ 91 s.
[394] Cfr. O. Mazza, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, cit., p. 12.

Con riferimento, invece, alla questione concernente la necessità, in una società democratica, di far uso di siffatti strumenti o elementi di prova, è stato evidenziato come in effetti l'art. 189 c.p.p. possa al più circoscrivere e limitare il loro ricorso se «utile» o «opportuno»[395], mentre il *case-law* convenzionale ha escluso che possa farsi riferimento a limiti dotati di un tale margine di «*discretion or* (…) *appreciation*»[396].

4. Il riconoscimento facciale nel quadro normativo sovranazionale

Si ritiene utile a questo punto presentare una breve panoramica sul quadro normativo, attualmente esistente in ambito sovranazionale, avente ad oggetto la specifica regolamentazione dell'impiego a fini giudiziari degli *automated facial recognition systems*[397]. Come anticipato *supra*, nell'ambito dell'Unione europea e, più in generale, a livello sovranazionale, si registra - ormai da qualche tempo - una diffusa consapevolezza circa l'utilità dell'impiego di tecniche di intelligenza artificiale (da qui in avanti IA) a servizio della giustizia[398]. Più specificamente, a partire dalla pubblicazione del «*Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*» del febbraio 2020[399], la Commissione europea ha evidenziato le potenziali implicazioni per i diritti fondamentali derivanti dall'impiego a distanza di sistemi di riconoscimento biometrico e, più in particolare, della tecnologia di riconoscimento facciale[400]. L'impiego di quest'ultima può essere concesso soltanto quando debitamente motivato, proporzionato e soggetto a garanzie adeguate. Per prevenire eventuali violazioni di diritti fondamentali, poi, la Commissione europea ha proposto di identificare le specifiche circostanze di tempo e di spazio che potrebbero giustificare tale uso, e alcune garanzie da adottare. Pochi mesi prima della pubblicazione del *White Paper*, peraltro, l'*High-Level Expert Group on AI* (AI HLEG), composto da esperti indipendenti e provenienti dall'ambito accademico e dall'industria, nel documento *Ethics Guidelines for Trustworthy AI*, ha posto in luce la necessità di introdurre una chiara definizione dei casi in cui può essere impiegata l'IA finalizzata al riconoscimento

[395] Cfr. C. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato*, cit., p. 16.
[396] Cfr. C. Edu, *Dudgeon c. the Regno Unito*, 22.10.1981, 21.
[397] Per una panoramica generale sul quadro normativo in materia di strumenti di intelligenza artificiale v. *supra* il capitolo III, § 2.1.
[398] Cfr. M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra stati uniti ed Europa*, cit., p. 12 e M. Caianiello, *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 29, (2021), p. 1.
[399] Cfr. il capitolo III, § 2.1.
[400] Cfr. COMMISSIONE EUROPEA [COM (2020,) 65 final], *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, consultabile sul sito internet della Commissione (ultimo accesso il 20.1.2022), p. 24.

automatizzato degli individui e la precisa distinzione fra «*identification of an individual, versus the tracing and tracking of an individual, and between targeted surveillance and mass surveillance*»[401].

Entro tale scenario, la Commissione europea, nella sua valutazione d'impatto che accompagna la proposta di regolamento sull'IA[402], ha messo a fuoco diversi livelli di precisione nelle prestazioni dei sistemi di *facial recognition* che potrebbero potenzialmente portare a determinati risultati discriminatori, individuandone un possibile contesto di regolamentazione[403].

Dal canto suo, il Parlamento europeo negli ultimi anni ha chiesto più volte di limitare, se non, addirittura vietare in determinate circostanze[404], l'impiego di siffatti strumenti. Più nel dettaglio, l'istituzione ha evidenziato che la raccolta e l'uso a distanza di dati biometrici per scopi di identificazione (in cui rientrerebbero certamente i sistemi di riconoscimento facciale) in spazi aperti al pubblico comporta rischi rilevanti per i diritti fondamentali[405]. A tal proposito, il Parlamento ha invitato altresì la Commissione a considerare l'introduzione di una moratoria sull'uso di questi sistemi negli spazi pubblici, nei luoghi di istruzione e della sanità, finché «*the technical standards can be considered fully fundamental rights-compliant, the results derived are non-biased and non-discriminatory, and there are strict safeguards against misuse that ensure the necessity and proportionality of using such technologies*»[406].

Nell'ambito del Consiglio d'Europa, invece, come già anticipato *supra*[407], dapprima con lo studio "*Algorithms and Human Rights*"[408] e, successivamente, con la "*Carta etica europea per l'uso*

[401] Cfr. HIGH-LEVEL EXPERT GROUP ON AI, *Ethics guidelines for trustworthy AI*, 2019, p. 33, reperibili all'indirizzo https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (visualizzato in data 20.1.2022).

[402] Si tornerà in modo più approfondito *infra*, al § 4.4.

[403] Cfr. EUROPEAN COMMISSION, *Impact Assessment accompanying the Proposal for an AI-framework*, 2021, p. 19, reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SC0084 (visualizzato in data 20.1.2022).

[404] Cfr. EUROPEAN PARLIAMENT, *Resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector*, 2020/2017(INI), reperibile all'indirizzo https://www.europarl.europa.eu/doceo/document/TA-9-2021-0238_EN.html (visualizzato in data 20.1.2022). Cfr. anche la richiesta alla Commissione europea da parte di un centinaio di membri del Parlamento europeo di sancire espressamente il divieto della sorveglianza biometrica di massa negli spazi pubblici, *MEPs' Letter to the European Commission*, 8.3.2021, reperibile all'indirizzo https://edri.org/wp-content/uploads/2021/03/MEP-Letter-on-AI-and-fundamental-rights-1.pdf (visualizzato in data 20.1.2022).

[405] Cfr. EUROPEAN PARLIAMENT, *Resolution on a framework of ethical aspects of artificial intelligence, robotics and related technologies*, 2020/2012(INL), reperibile all'indirizzo https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html (visualizzato in data 20.1.2022).

[406] Cfr. EUROPEAN PARLIAMENT, *Resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice*, 2020/2013(INI), reperibile all'indirizzo https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html (visualizzato in data 20.1.2022). Il contenuto della Risoluzione citata è stato recentemente ribadito in un'altra Risoluzione del Parlamento europeo, cfr. EUROPEAN PARLIAMENT, *Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters* (2020/2016(INI)), reperibile all'indirizzo https://www.europarl.europa.eu/doceo/document/TA-9-2021-10-06_EN.html#sdocta2 (visualizzato in data 20.1.2022).

[407] Cfr. il capitolo II, § 2.1.

[408] Reperibile all'indirizzo https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5 (visualizzato in data 13.5.2021).

dell'intelligenza artificiale nei sistemi di giustizia"[409], sono state proposte alcune riflessioni sulla tenuta dei principi di presunzione di innocenza, di parità delle armi e del contraddittorio a fronte dell'impiego di sistemi di intelligenza artificiale. Più specificamente, nel gennaio 2021 sono state pubblicate le *Guidelines on Facial Recognition*[410], basate sui principi della Convenzione 108+[411], che forniscono una serie di misure di riferimento che governi, sviluppatori di sistemi di riconoscimento facciale, produttori, aziende e pubbliche amministrazioni dovrebbero adottare per garantire che l'impiego di queste tecnologie non pregiudichi la dignità della persona, i diritti umani e le libertà fondamentali[412].

Sembra dunque che gli sforzi pressoché unanimi compiuti sia nell'ambito dell'Unione europea, sia in quello del Consiglio d'Europa, siano tesi verso un impiego sempre più consapevole delle nuove tecnologie, al fine di promuovere l'eccellenza nell'IA e le sue applicazioni virtuose, nel rispetto dei diritti fondamentali dell'individuo.

Dopo aver presentato alcune riflessioni sugli istituti e sui principi aventi ad oggetto la protezione dei dati entro i quali deve collocarsi l'impiego di queste tecnologie, l'analisi proseguirà nella disamina dei documenti normativi maggiormente rilevanti al fine di evidenziare la relativa efficacia e i limiti che essi manifestano.

4.1. *Facial recognition technology* e direttiva 2016/680/UE

Il punto di partenza può essere senz'altro individuato nella direttiva 2016/680/UE, avente ad oggetto, come già visto diverse volte in precedenza[413], il trattamento dei dati personali da parte delle autorità, a fini di prevenzione, investigazione e repressione dei reati (da qui in avanti LED)[414]. Seguendo l'ordine dei principi disciplinati mano a mano nelle diverse disposizioni della direttiva e che interessano ai fini del presente capitolo, non si può non fare cenno all'art. 4, che stabilisce che il trattamento dei dati personali - incluse, quindi, le rappresentazioni digitalizzate dei volti e i loro

[409] Cfr. CEPEJ - *European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment*, reperibile su https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment (visualizzato in data 22.4.2021).

[410] Cfr. COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA - CONVENTION 108, *Guidelines on Facial Recognition*, 2021, T-PD(2020)03rev4, reperibili all'indirizzo https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 (visualizzato in data 18.1.2022).

[411] Cfr. il capitolo IV, § 1.5.

[412] Per un approfondimento cfr. *infra*, il § 4.2.

[413] Cfr. il capitolo I § 1.1, il capitolo II § 1.5.1.1, il capitolo III § 2.4.

[414] Cfr. la direttiva 2016/680/UE del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla 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, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (o *Law Enforcement Directive*) reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016L0680. La direttiva 2016/680 è stata recepita a livello interno con il d.lgs. 18 maggio 2018 n. 51 reperibile all'indirizzo https://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/sg.

templates - deve avvenire in modo lecito, corretto e trasparente nonché seguire una finalità specifica, esplicita e legittima (definita in modo chiaro nel diritto degli Stati membri o dell'Unione)[415]. Pertanto, affinché il trattamento di suddetti dati sia «*lawful*», è necessaria una «*specific legal base*»[416]. Dal momento che i sistemi automatizzati di riconoscimento facciale hanno ad oggetto dati biometrici che rientrano nella categoria di particolari dati personali, in conformità con quanto stabilito dall'art. 3(13) LED e 4(14) del regolamento (UE) 2016/679 (da qui in avanti GDPR), occorre che siano altresì rispettati i requisiti descritti e disciplinati dall'art. 10 LED. Come visto *supra*[417], quest'ultimo prescrive che il trattamento dei dati è consentito solo se considerato «strettamente necessario» e soltanto se «autorizzato dal diritto dell'Unione o dello Stato membro» per «salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica», ovvero «se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato»[418]. Entro il contesto della direttiva, «*police departments typically invoke criminal procedure codes*», oppure i «*surveillance codes and police laws*», come loro specifica base legale per il trattamento dei dati impiegati in un software di riconoscimento facciale[419]. Tuttavia, come già emerso in precedenza[420], non sempre le disposizioni contenute nei codici di procedura penale o nelle leggi nazionali possono considerarsi effettivamente «*specific*» nei diversi passaggi della cd. "*biometric chain of custody*"[421].

Strettamente connesso al tema della legittimazione dell'impiego dei sistemi di riconoscimento in parola è il principio di proporzionalità[422], la cui valutazione - come noto ormai - dev'essere eseguita

[415] Cfr. il considerando n. 26 e l'art. 4 LED.
[416] Cfr. il considerando n. 35 LED. Cfr. altresì il capitolo I, § 1.1.
[417] Cfr. il capitolo I, § 1.1.
[418] Cfr. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., p. 24, EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Regulating facial recognition in the EU*, cit., p. 11, GRUPPO DI LAVORO – ARTICOLO 29, *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, cit., pp. 7-6.
[419] In alcune attività di sperimentazione di alcuni strumenti tecnici la base legale è stata individuata nel consenso da parte degli interessati. Cfr. BUNDESPOLIZEIPRÄSIDIUM POTSDAM, *Abschlussbericht Biometrische Gesichtserkennung*, 28 September 2018, pp. 22-23, reperibile all'indirizzo https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf?__blob=publicationFile (visualizzato in data 18.1.2022).
[420] Cfr. il capitolo I, § 1.1, il capitolo III, § 2.4 e il capitolo IV, §§ 2.1.1. e 3.1.3. Peraltro, oltre all'Autorità Garante italiana per la protezione dei dati personali (cfr. il § 2.1.1), anche l'*Hamburg Data Protection Authority* (DPA), in seguito all'impiego da parte delle autorità di polizia di una tecnologia in grado di estrarre dati biometrici in occasione del G20, ha stabilito che la base legale indicata per il suo utilizzo era «*unspezifische*». Cfr. *Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg*, Hamburg DPA, 31.8.2018, pp. 9-27, reperibile all'indirizzo https://datenschutz-hamburg.de/pressemitteilungen/2018/08/2018-09-31-polhh-g20-videmo360 (visualizzato in data 18.1.2022).
[421] Si ricorda la recente pronuncia della *Civil Division* della *Court of Appeal* d'oltremanica, approfondita poc'anzi (cfr. *supra* il § 3.1.3), in cui il quadro giuridico qualificato come base legale per l'impiego delle *AFR Locate* è stato giudicato impreciso dal momento che, inter alia, concedeva un margine di discrezionalità troppo ampio in capo alla *South Wales Police* nella predisposizione e nell'inserimento dei dati all'interno delle cd. *watchlists*. Cfr. [2020] EWCA Civ. 1058, §§ 90 – 96.
[422] Cfr. gli artt. 5, 8,10 LED e il considerando 26 LED.

caso per caso, tenendo conto della limitazione dei diritti, dello scopo e del contesto di impiego[423]. Per vero, la proporzionalità va valutata rispetto all'idoneità degli atti compiuti dai pubblici poteri per realizzare gli scopi perseguiti dalle norme, senza che ne siano travalicati i limiti[424]. A tal proposito, nel caso *Bridges* la *Court of Appeal* inglese ha stabilito che l'impiego da parte delle autorità di polizia dell'*AFR Locate* fosse certamente rispondente al principio di proporzionalità, ma in ogni caso «*unlawful*», dal momento che «*the "law" for the purposes of Article 8(2) is on further analysis insufficient*»[425].

Il trattamento dei dati, poi, deve essere «trasparente nei confronti della persona fisica interessata»[426]. Tuttavia, questo non deve impedire di per sé alle autorità competenti[427] di svolgere attività quali operazioni di infiltrazione o videosorveglianza, che possono essere eseguite, prosegue il considerando 26, «a fini 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». A tal proposito, l'art. 13 par. 3 LED stabilisce che gli Stati membri «possono adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato», al fine di evitare di ostacolare o, addirittura, pregiudicare le indagini in corso o la sicurezza nazionale. Tuttavia, è stato evidenziato come tali deroghe possano rivelarsi «*instrumental for law enforcement*»[428], precludendo così, ai diretti interessati, l'esercizio dei loro diritti. Ulteriore problematica applicativa concerne gli esatti confini del diritto dell'interessato a ricevere una spiegazione in seguito ad una valutazione algoritmica che lo riguardi, incluse le «*meaningful information about the logic involved*»[429]. Tale diritto può ragionevolmente essere applicato nel contesto delle tecniche automatiche di riconoscimento facciale, ma ancora una volta la sua attuazione rimane ad oggi piuttosto incerta.

Quanto alla *fairness*, si ritiene sufficiente ricordare che, sebbene il suo contenuto normativo risulti al centro di una disputa dottrinaria[430], il principio dovrebbe essere pensato come un *leitmotiv* vincolante per gli sviluppatori e per gli operatori nella fase di sviluppo e di progettazione dei piani di implementazione[431].

---

[423] In questo senso, occorre tenere bene distinte le finalità preventive e investigative nell'utilizzo di questi *tools* da parte della autorità di *law enforcement*.

[424] Cfr. C-293/12 e C-594/12, *Digital Rights Ireland*, CJEU, 8.4.2014 e C-203/15, *Tele2 Sverige*, CJEU, 21.12.2016.

[425] Cfr. [2020] EWCA Civ. 1058, § 90.

[426] Cfr. il considerando n. 26 LED.

[427] Cfr. l'art. 3 § 7 LED.

[428] Cfr. EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Regulating facial recognition in the EU*, cit., p. 13.

[429] Cfr. gli artt. 11, 13 e 14 LED e il considerando 38 LED. Per un approfondimento v. *supra* il capitolo II, § 2.2 e F. Palmiotto, *The Right to Contest Automated Decisions*, 14.2.2022, reperibile all'indirizzo https://digi-con.org/the-right-to-contest-automated-decisions/ (visualizzato in data 21.2.2022).

[430] Cfr. EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Regulating facial recognition in the EU*, cit., p. 13.

[431] Cfr. EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Regulating facial recognition in the EU*, cit., p. 13.

Particolarmente rilevante è poi l'articolo 4, par. 1, lett. *b*) della direttiva che disciplina il principio di "*limitazione delle finalità*", stabilendo la necessaria definizione di uno scopo preciso al momento della raccolta dei dati e che tali dati non siano riutilizzati per altro scopo incompatibile. Le immagini digitali dei volti risultano agevolmente collezionabili e i software di riconoscimento facciale richiedono l'elaborazione di una grande quantità di dati talché sia l'individuo direttamente interessato, sia il titolare del trattamento difficilmente potrebbero controllare un loro riutilizzo al momento della raccolta. Questo implica che le forze di polizia debbano applicare tale principio in tutte le fasi del procedimento penale, con la garanzia di un legame costante tra il titolare dei dati e il preciso scopo del trattamento. In tal senso, con riferimento a quest'ultimo principio, l'Agenzia dell'UE per i diritti fondamentali ha suggerito che le finalità di interesse pubblico per le quali risulti necessario il ricorso alle tecniche automatiche di riconoscimento facciale debbano essere in ogni caso «*strictly determined*»[432].

Ulteriore principio delle informazioni trattate tramite un software di riconoscimento facciale è quello della "*minimizzazione dei dati*"[433]. La *ratio* di base è costituita dalla limitazione della raccolta dei dati personali, entro i quali si riconducono altresì quelli biometrici, necessari per il raggiungimento della finalità consentita dalla legge, cancellando quelli non essenziali o non conformi allo scopo preposto. Tuttavia, come già anticipato *supra* rispetto ai dati biometrici *tout court*[434], risulta controverso come il principio di minimizzazione dei dati possa ragionevolmente conciliarsi con l'applicazione di tecniche di *machine learning* che, come visto nei precedenti paragrafi[435], richiedono per un loro corretto funzionamento una rilevante quantità di dati da processare[436]. Con specifico riferimento agli *automated face based human recognition systems, l'European Data Protection Board* ha aggiunto che «*data controllers must ensure that data extracted from a digital image to build a template will not be excessive and will only contain the information required for the specified purpose, once a facial template has been generated, the underlying raw data may need to be deleted*»[437].

L'art. 4, par. 1, lett. *d*) LED, poi, disciplina il "*principio di accuratezza*" dei dati, prevedendo che essi siano «esatti e, se necessario, aggiornati (…) rispetto alle finalità per le quali sono trattati». Come

[432] Cfr. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27.11.2019, p. 25.
[433] Cfr. l'art. 4, par. 1, lett. *c)* LED.
[434] Cfr. il capitolo I, § 1.1.
[435] Cfr. il capitolo III, §§ 2 e ss.
[436] Cfr. M. Ebers, *Regulating AI and Robotics: Ethical and Legal Challenges*, in AA.VV., *Algorithms and Law*, (a cura di) M. Ebers, S. Navas Navarro, Cambridge University Press, Cambridge, 2020, p. 64 e T. Taulli, *Artificial Intelligence Basics*, Apress, Berkeley, 2019, p. 36.
[437] Cfr. EUROPEAN DATA PROTECTION BOARD, *Guidelines 3/2019 on processing of personal data through video devices*, 2020, p. 21, reperibile all'indirizzo https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en (visualizzato in data 18.1.2022).

si approfondirà meglio *infra*[438], secondo le recenti *Guidelines on Facial Recognition* del Consiglio d'Europa, gli sviluppatori dei software sono tenuti a «*avoid mislabelling, thereby sufficiently testing their systems and identifying and eliminating disparities in accuracy, notably with regard to demographic variations in skin colour, age and gender, and thus avoid unintended discrimination*»[439]. Tuttavia, si ritiene che anche in questo caso l'applicazione empirica del principio sia piuttosto complessa e la questione non è stata ancora risolta[440].

In base al "*principio di sicurezza*" dei dati, il trattamento deve avvenire in modo da garantire la massima tutela contro la perdita, la distruzione o il danneggiamento accidentale dei dati[441]. Più nel dettaglio, il responsabile del trattamento è tenuto ad adottare diverse misure durante la trasmissione e la conservazione dei dati, come, per esempio, conservare i modelli biometrici e i dati grezzi in banche dati distinte, definire una politica di cifratura dei modelli elettronici biometrici e di gestione delle chiavi, integrare determinate misure per l'individuazione delle frodi, associare un codice di integrità ai dati e vietare qualsiasi accesso esterno alle informazioni trattate[442].

Secondo il "*principio di* accountability", invece, il responsabile del trattamento dei dati è tenuto a dimostrare il rispetto dei principi posti a tutela degli stessi[443]. Per l'impiego di strumenti di riconoscimento facciale è necessaria la predisposizione di una valutazione d'impatto sulla protezione dei dati, compresa la consultazione preventiva dell'autorità garante nazionale[444]. Il responsabile del trattamento deve poi registrare le attività di gestione delle informazioni trattate[445] e conservare i documenti che attestino l'avvenuta violazione delle norme poste a tutela dei dati[446].

Coerentemente con l'interpretazione giurisprudenziale della Corte di giustizia[447], poi, si autorizza il trattamento dei dati biometrici entro la cui categoria è possibile ricondurre la rappresentazione digitalizzata o il *template* di un volto ricavata da un'immagine o da un *frame* di un filmato di videosorveglianza, purché sia «strettamente necessario», ossia in presenza di giustificazioni precise e particolarmente rilevanti per il trattamento di tali dati, ovvero che lo stesso sia «autorizzato dal diritto»

---

[438] Cfr. *infra* il § 4.2.

[439] Cfr. COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA - CONVENTION 108, *Guidelines on Facial Recognition*, 2021, T-PD(2020)03rev4, p. 9, reperibili all'indirizzo https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 (visualizzato in data 18.1.2022).

[440] Cfr. EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Regulating facial recognition in the EU*, cit., p. 16.

[441] Cfr. l'art. 4, par. 1, lett. *f*) LED.

[442] Cfr. EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Regulating facial recognition in the EU*, cit., p. 17.

[443] Cfr. l'art. 4, par. 4 LED.

[444] Cfr. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, cit., p. 26; INFORMATION COMMISSIONER'S OFFICE, *Opinion on the use of live facial recognition technology by law enforcement in public places*, 2019, cit., pp. 13-14; EUROPEAN DATA PROTECTION BOARD, *Guidelines 3/2019 on processing of personal data through video devices*, cit., 2020, p. 33.

[445] Cfr. l'art. 24 LED.

[446] Cfr. l'art. 30 par. 5 LED.

[447] Cfr. *ex multis*, C-293-12 e C-594/12, *Digital Rights Ireland v. Minister for Communications e.a.*, cit., p. 52.

dell'UE o degli Stati, o che sia «soggetto a garanzie adeguate per i diritti e le libertà dell'interessato»[448]. Trattasi di condizioni e garanzie poste a tutela dell'individuo destinatario che lasciano agli Stati membri ampi margini di azione. Basti considerare solo che, sul versante italiano, il d.P.R. 15/2018, attuativo del d.lgs. 196/2003[449], ha previsto - molto genericamente - che il trattamento dei dati biometrici sia consentito «quando è necessario per le esigenze di un'attività informativa, di sicurezza o di indagine di polizia giudiziaria o di tutela dell'ordine e della sicurezza ad integrazione di altri dati personali»[450]. Questo però non può considerarsi sufficiente. Si ribadisce nuovamente la necessità di introdurre una regolamentazione nazionale chiara, prevedibile e adeguatamente accessibile, al fine di consentire alle persone interessate di agire in conformità alla legge e delimitare chiaramente la portata della discrezionalità delle autorità pubbliche.

Infine, come già accennato *supra*[451], l'art. 11 della direttiva in esame prescrive il divieto per gli Stati membri di dare esecuzione a decisioni basate unicamente su un trattamento automatizzato che produca effetti giuridici negativi o incida significativamente sui diritti fondamentali dell'interessato, salvo il caso in cui sia autorizzata dal diritto dell'Unione o dello Stato membro, cui è soggetto il titolare del trattamento, e che preveda garanzie adeguate per il diritto di ottenere l'intervento umano da parte del titolare del trattamento[452]. La previsione di una verifica del risultato scaturente dal *tool*, da parte di un operatore specializzato (pur nella fase finale dell'attività dello strumento), costituisce in ogni caso «una salvaguardia di importanza fondamentale per i diritti dei singoli»[453]: l'intervento umano è, infatti, una garanzia importante, in grado di ridurre (ma non di eliminare) la probabilità che un soggetto subisca un errore valutativo da parte dell'algoritmo. Tuttavia, in assenza di una regolamentazione compiuta delle diverse fasi della "*biometric chain of custody*", sorge spontaneo chiedersi come può essere possibile l'esercizio di una qualche forma di controllo del fatto che tali verifiche "manuali" siano effettivamente state poste in essere e le diverse metodologie scientifiche siano state applicate correttamente.

---

[448] Così l'art. 10 della LED.

[449] Emanato contestualmente al d.lgs. 51/2018, attuativo della direttiva UE/2016/680. Cfr. il capitolo I, § 1.1.

[450] Cfr. l'art. 11, c. 2 del d.P.R. n. 15/2018.

[451] Cfr. il capitolo III, § 2.1.

[452] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, p. 196.

[453] «Si tratta quest'ultima, di una garanzia chiave, la quale – tra l'altro – impedisce di poter qualificare le decisioni prese mediante il meccanismo in esame "totalmente automatizzate" ai sensi dell'art. 11 della direttiva 2016/680/UE; e ciò in quanto un essere umano è sempre coinvolto nella fase finale di utilizzo dello strumento». Cfr. J. Della Torre, *Novità dal regno unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del garante privacy d'oltremanica)*, in *www.sistemapenale.it*, 28.3.2020, p. 242.

4.2 Le Linee Guida del Consiglio d'Europa sull'uso del riconoscimento facciale nel settore pubblico e privato T-PD(2020)03rev4

In data 28 gennaio 2021, nell'ambito del Consiglio d'Europa, sono state emanate le linee guida per l'uso del riconoscimento facciale nel settore pubblico e privato[454]. Il documento è stato stilato dal Comitato consultivo della Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati personali, che riunisce esperti dei 55 Stati contraenti la Convenzione e 20 Stati osservatori. La *ratio* di base dell'intero documento è che le parti della c.d. Convenzione 108+ devono essere in grado di garantire che l'impiego degli *automated facial recognition systems* rispetti i diritti alla vita privata e la protezione dei dati, rafforzando in tal modo i diritti umani e le libertà fondamentali[455].

L'attenzione del Consiglio d'Europa per il crescente impiego di strumenti digitali governati, in generale, da algoritmi e forme più o meno sofisticate di intelligenza artificiale, in tutti i settori delle istituzioni, anche quelle giudiziarie, è ormai nota. Già nel marzo del 2018, veniva pubblicato l'interessante studio dal titolo "*Algorithms and Human Rights*"[456], nella cui sezione dedicata a *fair trail* e *due process* si anticipavano alcune delle preoccupazioni affrontate solo successivamente nella Carta etica europea per l'uso dell'IA nella giustizia e[457], ancora dopo, dalla Commissione europea con il "Libro bianco sull'intelligenza artificiale"[458].

Il documento in esame è rivolto in maniera indistinta a soggetti pubblici e privati, a vario titolo coinvolti nella realizzazione e nell'utilizzo di strumenti di intelligenza artificiale, aventi lo scopo di elaborare automaticamente le immagini digitalizzate contenenti i volti di individui per il riconoscimento o la verifica dell'identità. Le linee guida si rivolgono anche ai legislatori chiamati a stabilire una cornice normativa entro la quale tali strumenti debbano essere sviluppati, verificati e utilizzati, al fine di garantire che il loro impiego non incida negativamente sulla dignità umana, i diritti umani e le libertà fondamentali, compreso il diritto alla protezione dei dati personali[459]. Ma v'è di più.

---

[454] Cfr. COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA - CONVENTION 108, *Guidelines on Facial Recognition*, 2021, T-PD(2020)03rev4, reperibili all'indirizzo https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. Per un primo commento sul documento v. C. Jasserand, *New Extensive Guidelines on the Use of Facial Recognition by the Council of Europe*, in *EAB's Newsletter*, 2021.

[455] La Convenzione, già menzionata *supra* nel capitolo II § 1.5, è stato uno dei primi trattati internazionali vincolanti ad affrontare la necessità di proteggere i dati personali, aperto alla firma a Strasburgo 40 anni fa, il 28 gennaio 1981. Reperibile su all'indirizzo https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078c45.

[456] Cfr. il capitolo II, § 2.1.

[457] Reperibile su https://www.coe.int/en/web/cepej/special-file-publication-2018-edition-of-the-cepej-report-european-judicial-systems-efficiency-and-quality-of-justice- (visualizzato in data 18.1.2022).

[458] Reperibile su https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence (visualizzato in data 18.1.2022).

[459] Cfr. COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA - CONVENTION 108, *Guidelines on Facial Recognition*, cit., p. 4.

Il documento chiede di adottare un livello superiore di tutela per l'individuo specificando che «*using digital images that were uploaded on the Internet, including social media or online photo management websites or were captured passing through the lens of video surveillance cameras cannot be considered lawful on the sole basis that the personal data were made manifestly available by data subjects*». Per questa ragione, i legislatori nazionali «*have to lay down specific rules for biometric processing by facial recognition technologies for law enforcement purposes. These laws will ensure that such uses must be strictly necessary and proportionate for these purposes and prescribe the necessary safeguards to be provided*»[460]. Questo costituisce un primo punto essenziale da porre in luce nell'individuazione degli obiettivi del testo: non c'è più tempo da perdere, gli strumenti di riconoscimento facciale necessitano di una regolamentazione sì elastica, ma precisa. In particolare, poi, specifica attenzione viene data al categorico divieto di utilizzo di strumenti automatici di riconoscimento facciale aventi lo scopo di determinare il colore della pelle, le convinzioni religiose o di altro tipo, il sesso, l'origine razziale o etnica[461].

All'interno della cornice costituita dalla Convenzione 108+ e delle specifiche garanzie enunciate nelle linee guida, il Consiglio d'Europa mostra invece una certa apertura verso strumenti che possono determinare un aumento dell'efficienza complessiva dei sistemi di giustizia. A tal proposito, si ritiene fondamentale mantenere un costante approccio multidisciplinare nello sviluppo, nella verifica e nell'applicazione di strumenti computazionali, affinché essi possano davvero rappresentare un'evoluzione nell'efficienza della giustizia e non un elemento di rischio per le garanzie fondamentali degli individui.

Nonostante il saldo auspicio di dialogo fra diverse discipline, si riscontra già una prima problematica nella premessa del documento, ove, come in altri documenti normativi[462], i dati biometrici sono definiti come «*data uniquely identifying a person*»[463]. Dal punto di vista forense, questo costituisce un equivoco rilevante, che addossa ai tratti fisici, fisiologici o comportamentali così considerati l'incarico di identificare univocamente un individuo[464]. Come già visto *supra*, l'attività di comparazione automatica fra due volti eseguita tramite software si esprime soltanto in termini di similarità tra due dati e non di univocità. Questo è un punto fondamentale che si deve cominciare a

[460] Cfr. COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA - CONVENTION 108, *Guidelines on Facial Recognition*, cit., p. 2.

[461] Cfr. COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA - CONVENTION 108, *Guidelines on Facial Recognition*, cit., p. 5.

[462] Cfr. il capitolo I, § 1.

[463] Cfr. COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA - CONVENTION 108, *Guidelines on Facial Recognition*, cit., p. 3.

[464] Si ritiene, invece, opportuna la definizione di "*facial recognition*", inteso come «*the automatic processing of digital images containing individuals' faces for identification or verification of those individuals by using face templates*». Per un approfondimento sulle finalità di "*identification*" e "*verification*" nella disciplina biometrica cfr. il capitolo I, § 2.4.

tenere in considerazione anche per evitare di riporre false speranze nelle effettive capacità tecniche di uno strumento automatico di riconoscimento.

Ulteriore riflessione di carattere generale, poi, riguarda il costante riferimento ai *templates* biometrici. Si è già avuto modo di sottolineare che, per il funzionamento della maggioranza delle banche dati oggi in uso alle forze di polizia, è ormai sufficiente l'impiego della semplice rappresentazione digitale del volto, senza che debba essere espletato il successivo passaggio di conversione dell'immagine in *template*[465]. Certamente è possibile che le due tecnologie continuino a convivere per un lasso di tempo indeterminato, ma resta fermo, in ogni caso, che le tecniche di *machine learning* permettono ormai di estrapolare, analizzare e comparare le immagini digitali automaticamente già da diverso tempo.

Giova a questo punto passare in rassegna brevemente ciascuno dei principi sanciti nel documento.

4.2.1. I principi di trasparenza e *fairness*

Sancendo i principi di trasparenza e *fairness*, si raccomanda che siano fornite ai singoli tutte le informazioni tra le quali, il contesto di raccolta, le finalità per cui i dati saranno utilizzati, il potenziale impatto sui diritti fondamentali degli individui rispetto alla raccolta, all'impiego e alla condivisione dei dati relativi al riconoscimento facciale[466]. Le informazioni sull'impiego dei software automatici dovranno essere comprensibili e riportare le dovute indicazioni circa la finalità di trattamento, l'autorità che utilizza la tecnologia e la durata. Esse dovranno essere apposte nelle vicinanze appropriate del luogo in cui tali strumenti sono impiegati. L'uso occulto di tecnologie di riconoscimento facciale "*live*" da parte delle autorità di pubblica sicurezza rimane consentito solamente se ritenuto strettamente necessario e proporzionato per prevenire un rischio imminente e sostanziale per la sicurezza pubblica.

Con riferimento al campo della giustizia, poi, tenendo conto che i sistemi automatici di riconoscimento facciale si basano su tecniche di intelligenza artificiale, non è chiaro se chi si serve di questi strumenti dovrà garantire altresì l'accessibilità, la comprensibilità e la verificabilità esterna dei processi computazionali utilizzati. Si è già più volte fatto cenno al complesso rapporto tra la protezione della proprietà intellettuale e del *trade secret* e la necessità di osservare e criticare i processi computazionali utilizzati[467]. La preoccupazione si riferisce all'intero settore pubblico, ma assume un valore ancora più spiccato rispetto alla giustizia e, nell'ambito di questa, in particolare al processo

[465] Cfr. il capitolo I, 2.2.

[466] Cfr. COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA - CONVENTION 108, *Guidelines on Facial Recognition*, cit., p. 11.

[467] Cfr. il capitolo II, § 2.2.

penale, in cui sono in gioco i più elevati beni giuridici, come la libertà personale. A prescindere dalle soluzioni tecniche che, caso per caso, possono essere utilizzate per rispondere a specifiche esigenze che si presentino nel singolo procedimento, risulta ormai noto che il principio di trasparenza non rappresenta di per sé la "panacea" contro tutti gli squilibri generati dall'impiego di software automatici: anche quando il *reverse engeneering* sia possibile, infatti, la comprensione del modello può rimanere una questione limitata ai soli esperti, con esclusione degli effettivi destinatari del risultato automatizzato. Nel campo della giustizia penale, questo assume un significato particolare con riferimento all'ultima fase del procedimento probatorio, ossia la valutazione della prova. Infatti, a fronte della necessità da parte del giudice di motivare la valutazione di attendibilità di ciascuna prova, la trasparenza algoritmica - come visto - non risulta di per sé in grado di fornire al giudice e ai destinatari della decisione l'effettiva comprensione del calcolo che ha portato a generare un determinato risultato di compatibilità o meno fra due dati, lasciando nell'incertezza anche il giudizio sulla sua attendibilità. A tal proposito, l'opzione collaterale individuata dalle linee guida sarebbe costituita dalla predisposizione di autorità indipendenti che hanno il compito di verificare e certificare i modelli impiegati nei software, al fine di «*demonstrate full compliance of the processing operations*»[468].

4.2.2. Qualità e sicurezza dei dati

Un ulteriore monito sancito nel documento è costituito dalla garanzia di qualità e sicurezza con riferimento all'analisi dei dati. In particolare, l'impiego di sistemi di riconoscimento facciale dovrà evitare il più possibile le disparità di trattamento, soprattutto con riferimento alle variazioni demografiche del colore della pelle, dell'età e del genere, escludendo eventuali discriminazioni. Al fine di garantire sia la qualità dei dati sia l'efficienza dei sistemi di riconoscimento, gli algoritmi dovranno essere sviluppati utilizzando *set* di dati sintetici[469], basati su foto sufficientemente diversificate di uomini e di donne, di diversi colori della pelle, di diverse morfologie, di tutte le età e prese da angolazioni differenti. Viene specificato poi che i dati biometrici che rivelano altri dati sensibili, come informazioni su alcuni tipi di patologie e disabilità fisiche, dovrebbero essere soggetti

[468] Cfr. COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA - CONVENTION 108, *Guidelines on Facial Recognition*, cit., p. 8.

[469] Ossia «*algorithmically generated data, produced via reinforcement learning or generative adversarial networks (GANs)*», i quali «*offer an opportunity to address certain issues of data bias*». La definizione si trova in A. Tsamados, N. Aggarwal, J. Cowls et al., The ethics of algorithms: key problems and solutions, in *AI & Soc* 37, 2022, pp. 215–230. Sul punto cfr. anche A. Kortylewski, B. Egger, A. Schneider, T. Gerig, A. Morel-Forster, T. Vetter, *Analyzing and Reducing the Damage of Dataset Bias to Face Recognition With Synthetic Data*, in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, 2019, pp. 1-8 e L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Raffaello Cortina Editore, Milano, 2022, p. 71.

a garanzie complementari adeguate. Più nel dettaglio, un sistema di riconoscimento facciale richiede il rinnovo periodico dei dati (le immagini dei volti da riconoscere) al fine di istruire e migliorare l'algoritmo utilizzato. Ciascun algoritmo ha una percentuale di affidabilità di riconoscimento, sia durante il suo sviluppo sia durante il suo utilizzo. A tal proposito, le linee guida sottolineano l'importanza di conoscere tale percentuale per monitorare la sua evoluzione. Questo consentirà certamente anche la protezione dalle conseguenze delle modifiche nella forma dei volti (per es. dovute all'invecchiamento, agli accessori, a *piercing* o altri interventi).

Quanto all'affidabilità degli strumenti automatici, tale parametro dipende essenzialmente dalla qualità del *training* eseguito dall'algoritmo. Vi sono diversi fattori che incidono sul valore in esame, tra cui la percentuale di falsi positivi, di falsi negativi, delle prestazioni differenti a seconda del posizionamento della luce, ovvero della posizione dei volti. Le linee guida raccomandano un livello massimo rispetto al parametro di affidabilità, considerando che l'uso di un sistema di riconoscimento facciale potrebbe comportare conseguenze negative molto significative per l'individuo. La selezione dei dati da immettere nel procedimento di elaborazione implica un'attenta verifica dell'affidabilità della fonte e dell'integrità dell'informazione, per evitarne modificazioni accidentali o strumentali. Le imprese che sviluppano tecniche di riconoscimento facciale - proseguono le linee guida - dovrebbero adottare misure specifiche per garantire il rispetto dei principi di protezione dei dati, tra cui si ricordano la cancellazione automatica dei dati grezzi dopo l'estrazione dei modelli biometrici, il rispetto dei principi di limitazione delle finalità, la minimizzazione dei dati e la limitazione della durata di archiviazione degli stessi. Inoltre, viene sottolineata l'importanza di attuare un procedimento di revisione interno volto ad individuare e attenuare il potenziale impatto sui diritti e sulle libertà fondamentali prima che siano rese disponibili le tecnologie per il riconoscimento facciale.

4.2.3 Il principio di *accountability*

Sia gli enti pubblici sia quelli privati che utilizzano tecnologie di riconoscimento facciale devono effettuare valutazioni d'impatto prima del trattamento, poiché l'uso di tali tecnologie comporta l'elaborazione di dati biometrici che presenta rischi particolarmente elevati per i diritti fondamentali delle persone interessate[470]. Nell'ambito di tale valutazione d'impatto, dovrà essere stabilita la legittimità dell'uso di tali tecnologie, i diritti fondamentali in gioco nel trattamento biometrico e la

[470] Più nel dettaglio «*in the public sector: prior evaluation constraints in public procurement procedures involving suppliers of facial recognition tools, assessment of minimum levels of performance in terms of accuracy, especially where law enforcement purposes are concerned*». Cfr. COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA - CONVENTION 108, *Guidelines on Facial Recognition*, cit., pp. 13 e ss.

predisposizione di adeguate misure che riducano i rischi di possibili violazioni alla libertà di espressione, alla libertà di circolazione o con riferimento a eventuali risultati discriminatori. In particolare, le *Guidelines* specificano che «*entities using facial recognition technologies should ensure that human operators continue to play a decisive role in the actions taken upon the results of these technologies*». A loro volta, «*entities using these technologies should take organisational measures to oversee the human operators taking decisions which can have a significant impact on individuals*». Vien da domandarsi anche in questo caso[471] se, ai fini della determinazione dell'*accountability*, la predisposizione di queste cd. «*organisational measures*» possa essere considerata sufficiente per dare effettività e concretezza all'azione del Consiglio d'Europa in questo ambito. Il rischio è sempre quello di scambiare l'inserimento di una serie di criteri tecnici, anche estremamente dettagliati, senza stabilire gli effetti di eventuali trasgressioni, per una effettiva tutela dei diritti fondamentali dell'interessato.

4.2.4. Il ruolo dell'utente nell'impiego di software di riconoscimento facciale

L'ultimo monito enunciato dalle linee guida è il necessario controllo da parte dell'utente, al fine di garantire che gli utilizzatori agiscano come soggetti informati, nel pieno controllo delle loro scelte. Infatti, gli strumenti computazionali e i sistemi di intelligenza artificiale devono accrescere l'autonomia decisionale dell'utente e non ridurla. Tutti i diritti sanciti nell'articolo 9 della Convenzione 108+ sono garantiti alle persone interessate, tra cui «*the right of information, the right of access, the right to obtain knowledge of the reasoning, the right to object, the right to rectification*». Tali diritti possono essere limitati, ma solo quando una restrizione sia prevista espressamente dalla legge, costituendo una misura necessaria e proporzionata in una società democratica per scopi legittimi e specifici, ai sensi dell'art. 11 della Convenzione 108+.

4.3. Il "*Next generation Prüm*" e i possibili sviluppi del sistema di scambio e circolazione di dati

Si è fatto cenno *supra* ad alcuni degli strumenti normativi attualmente in vigore che regolano lo scambio di dati biometrici digitalizzati in un'ottica di cooperazione internazionale per la lotta alla criminalità grave ed al terrorismo[472]. Tra questi si è fatto brevemente cenno al cd. Trattato di Prüm, stipulato il 27 maggio 2005 tra Belgio, Germania, Spagna, Francia, Lussemburgo, Paesi Bassi e Austria, volto al rafforzamento della cooperazione tra gli Stati nella lotta al terrorismo, alla criminalità transfrontaliera e all'emigrazione illegale. L'accordo, *inter alia*, ha lo scopo di raccogliere e scambiare

[471] Cfr. il capitolo II, § 3.1.
[472] Cfr. il capitolo II, § 1.5.1.1.

informazioni relative ai profili o campioni del Dna, le impronte digitali e i dati relativi ai registri di immatricolazione dei veicoli[473]. A pochi anni di distanza dalla sua introduzione, come visto, sono state poi approvate le decisioni 2008/615/GAI e 2008/616/GAI che hanno integrato e attuato, nel quadro normativo europeo, le disposizioni del Trattato di Prüm[474].

Per far fronte alle difficoltà operative e alla eccessiva frammentarietà del quadro giuridico di riferimento[475], unitamente all'affermarsi di nuove tecniche e strumenti di indagine basati sul trattamento di dati personali, le istituzioni dell'Unione europea, in particolare la Commissione e il Consiglio, hanno di recente cominciato a promuovere iniziative legislative[476], studi e ricerche concernenti la modernizzazione delle decisioni di Prüm e del relativo meccanismo di scambio dei dati[477]. Tra i possibili interventi volti a innovare e modernizzare il regime esistente, un'area tematica risulta particolarmente rilevante ai fini della presente ricerca, ossia il possibile ampliamento delle categorie di dati rientranti nel meccanismo di scambio di Prüm. Uno studio elaborato da *Deloitte*, condotto nel maggio 2020, su richiesta della Commissione europea, ha considerato infatti la possibilità di inserire, insieme ai profili del Dna, ai dati dattiloscopici e a quelli relativi ai veicoli immatricolati, anche le rappresentazioni digitalizzate dei volti, finalizzate all'impiego di sistemi automatici di riconoscimento facciale[478]. La motivazione risiede nell'importanza e nell'utilità sempre più in crescita di tali informazioni a fini investigativi e probatori. Introducendo la previsione di uno scambio transfrontaliero di immagini facciali, si renderebbe possibile eseguire un riconoscimento biometrico impiegando informazioni contenute nelle banche dati di altri Stati membri. A tal proposito, il primo obiettivo da raggiungere sarebbe la creazione di banche dati nazionali contenenti le rappresentazioni

[473] Cfr. il capitolo II, § 1.5.1.2.
[474] Cfr. il capitolo II, § 1.5.1.2.
[475] Cfr. il capitolo II, § 1.5.1.2.
[476] Cfr. *Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council*, COM/2021/784 final, reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A784%3AFIN&qid=1639141496518.
[477] L'espressione "*Next generation Prüm*" è stata coniata dal Working Party on Information Exchange and Data Protection, un organo preparatorio del Consiglio, che ha iniziato a vagliare la possibilità di dar seguito al progetto in esame. Cfr. WORKING PARTY ON INFORMATION EXCHANGE AND DATA PROTECTION (DAPIX), 4.4.2017, reperibile all'indirizzo https://www.consilium.europa.eu/en/meetings/mpo/2017/4/working-party-on-information-exchange-and-data-protection-dapix-(255033)/ (visualizzato in data 19.1.2022). Per un primo commento sul tema V. L. Scaffardi, *Next Generation Prüm e le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, in *federalismi.it*, 8/2021, pp. 211 e ss., L. Scaffardi, *Forensic genetics: The evolving challenge of DNA cross-border exchange*, in *BioLaw Journal –Rivista di BioDiritto*, Special Issue 1(2021), pp. 329 e ss., e H. Machado, R. Granja, A. Amorim, *Ethical challenges of merging criminal identification and civil identification within the Prüm system*, in *Forensic Science International: Genetics*, Vol. 57, 2022.
[478] Cfr. COMMISSIONE EUROPEA, DIREZIONE GENERALE DELLA MIGRAZIONE E DEGLI AFFARI INTERNI, *Study on the feasibility of improving information exchange under the Prüm decisions: cost benefits analysis: final version*, Publications Office, 2020, reperibile all'indirizzo https://op.europa.eu/it/publication-detail/-/publication/503f1551-9efc-11ea-9d2d-01aa75ed71a1/language-en (visualizzato in data 19.1.2022).

digitali dei volti, analogamente a quanto stabilito dalle decisioni di Prüm per altre categorie di dati. Tali archivi sarebbero gestiti in modo autonomo da ciascuno Stato membro e dovrebbero contenere sia i dati biometrici di soggetti ignoti, sia di soggetti condannati o ricercati e, dunque, già noti alle autorità di *law enforcement*. Il modello di cooperazione proposto ricalcherebbe essenzialmente quello avente ad oggetto le altre tipologie di dati: a una prima trasmissione dell'immagine di un volto alle autorità competenti individuate da ciascuno Stato membro, seguirebbe l'esecuzione di un'operazione di *match*, ovvero di corrispondenza sulla base del meccanismo *hit/no hit*[479]. Nel caso di esito positivo di tale primo vaglio, sarà data esecuzione al trasferimento e alla condivisione delle informazioni personali dell'individuo da parte dello Stato membro il cui database contenga una immagine facciale che corrisponda a quella inoltrata dal Paese richiedente. Lo scambio delle rappresentazioni digitali o di *templates* di volti dovrebbe avvenire, poi, sulla base di una serie di linee guida, introdotte per garantire la qualità standard delle immagini da scambiare, predisponendo un numero minimo e massimo di *match* da trasferire e comunicare, fissando termini brevi per la conservazione dei dati inviati ad altri Stati membri per i quali non è stata riscontrata alcuna corrispondenza[480].

Tuttavia, sono emerse non poche perplessità per la realizzazione concreta di tale progetto normativo. In primo luogo, la maggior parte degli Stati membri non ha ancora le capacità e gli strumenti tecnici che consentano di supportare uno scambio sistematico di impronte facciali[481]. Permangono poi i rischi legati alla bassa qualità delle immagini condivise e di quelle inserite nei database e dell'algoritmo che regola le operazioni di confronto, il quale potrebbe essere affetto da *bias*, già a partire dalla sua progettazione[482]. Come è stato evidenziato, «*the degree of accuracy in facial recognition technology is vital, so as to minimise the risk of false positive matches, namely results that may be unrelated to the investigation, or false negative results, when the FR algorithm fails to identify correct matches. This is crucial since facial recognition technology will be used in the course of criminal investigations with the aim of identifying unknown perpetrators, therefore national authorities will perform searchers on the basis of a facial image (a mug shot or a probe retrieved from*

[479] Cfr. il capitolo II, § 1.5.1.2. Cfr. *Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council, COM/2021/784 final*, cit., artt. 22 e 23.

[480] Cfr. L. Scaffardi, *Next Generation Prüm e le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, cit., p. 217.

[481] Cfr. L. Scaffardi, *Next Generation Prüm e le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, cit., p. 216, ove l'Autrice sottolinea che «manca in quasi tutti gli Stati membri un *national central electronic image database* (un unico *repository* centralizzato di tutte le immagini facciali di soggetti sconosciuti e sospettati di aver commesso un reato nonché di soggetti condannati), sia di un *national Face Recognition software* in grado di consentire le operazioni di "riconoscimento facciale" vero e proprio, di confronto cioè delle immagini della banca dati con una specifica immagine catturata da una videocamera».

[482] Cfr. EDPS, *Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation* ("Prüm II"), 2.3.2022, p. 6.

a camera) against the full content of other national databases and the top results will be ranked. False positive matches in particular may have important consequences for individuals, who may be bothered by the police because of incorrect matching, be subject to criminal investigation and even be subject to discriminatory practices by national authorities»[483]. Pertanto, sebbene l'intervento umano sia in ogni caso considerato un potenziale correttivo del risultato scaturente dal software, i dubbi sulla reale efficacia di tale sistema e sul valore aggiunto che potrebbe essere dato al meccanismo di Prüm, con l'implementazione dello scambio delle immagini facciali, permangono[484]. Il dibattito circa l'inserimento dei volti nel meccanismo di scambio dei dati per finalità di indagine è dunque aperto. Ancora una volta, la preoccupazione maggiore rilevata nell'ambito dell'impiego di tecnologie di riconoscimento facciale è rappresentata proprio dalla sostanziale mancanza di una disciplina normativa di riferimento e dai potenziali rischi correlati all'impiego di strumenti ritenuti «ancora dai contorni opachi e per certi aspetti controversi e criticati»[485].

4.4. *Automated facial recognition technology* e la proposta di regolamento sull'intelligenza artificiale 2021/0106(COD)

Il vuoto legislativo attuale però sembra essere destinato ad esaurirsi in un futuro non così lontano. Come già approfondito più in generale *supra*[486], la Commissione europea ha di recente pubblicato una proposta di regolamento sull'intelligenza artificiale ("*Artificial Intelligent Act*") «che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione» (d'ora in poi "proposta")[487]. A tal proposito, la Commissione propone di distinguere nell'ambito dei sistemi di identificazione biometrica a distanza tra quelli impiegati "*in real time*" e in "*post remote*"[488],

[483] Cfr. POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS OF THE EUROPEAN PARLIAMENT, *Police Information Exchange - The future developments regarding Prüm and the API Directive*, 15.9.2020, p. 32, reperibile all'indirizzo https://www.europarl.europa.eu/thinktank/it/document/IPOL_STU(2020)658542 (visualizzato in data 19.1.2022).

[484] Cfr. POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS OF THE EUROPEAN PARLIAMENT, *Police Information Exchange - The future developments regarding Prüm and the API Directive*, 15.9.2020, cit., p. 33, «*contemporary research demonstrates that such searches are likely difficult due to an adequate quality of such images. If this option goes forward, the sources of facial images require clarity and data protection safeguards must be embedded so that the quality of facial images is high enough to prevent the risk of increased false matches, which may lead to discriminatory practices. The specific purposes for searching facial images should also be circumscribed so as to prevent wide-ranging surveillance practices at the national level*».

[485] Cfr. L. Scaffardi, *Next Generation Prüm e le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, cit., p. 223.

[486] Cfr. il capitolo II, § 2.1.1.

[487] Cfr. COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, COM/2021/206 final, reperibile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52021PC0206 (visualizzato in data 25.8.2021).

[488] V'è da ricordare che il Consiglio dell'Unione europea, nel primo testo di modifica delle disposizioni contenute nella proposta diffuso di recente, ha proposto di eliminare dalla definizione dei sistemi di riconoscimento biometrico l'aggettivo "remoti" per

sottoponendoli a una serie di regole diverse a seconda del loro utilizzo. Mentre tra i primi rientrano gli strumenti in grado di acquisire e confrontare dati biometrici istantaneamente (ovvero senza un ritardo significativo) e sulla base di materiale fornito in diretta o quasi in diretta, tra i sistemi impiegati in "*post remote*" si ricomprenderebbero quei *tools* che consentono il rilievo dei dati e le attività di confronto e riconoscimento con un ritardo significativo, sulla base di rappresentazioni digitalizzate di volti o filmati generati da telecamere a circuito chiuso (CCTV)[489]. Entro tale contesto, sono stati prospettati due diversi scenari per la regolamentazione del riconoscimento facciale.

Con riferimento ai sistemi "*real time*" di identificazione biometrica impiegati da autorità di *law enforcement*, in luoghi aperti al pubblico, in linea di principio la Commissione, come visto, propone di vietarne l'impiego[490]. Tali strumenti risultano particolarmente intrusivi e inferiscono gravemente con l'esercizio di diverse libertà fondamentali dei soggetti destinatari interessati. Oltre a ciò, secondo la Commissione, l'impiego di questi strumenti «potrebbe avere ripercussioni sulla vita privata di un'ampia fetta della popolazione, farla sentire costantemente sotto sorveglianza e scoraggiare in maniera indiretta l'esercizio della libertà di riunione e di altri diritti fondamentali»[491]. In ragione della potenziale lesività di tali *tools*, la Commissione li identifica come sistemi "ad alto rischio", il cui impiego da parte di autorità di *law enforcement* in spazi aperti al pubblico va generalmente vietato nello spazio euro-unitario. Nonostante questo, la Commissione ammette che tali sistemi possano essere anche di rilevante ausilio alle forze dell'ordine in contesti caotici e di grandi assembramenti, ma, trattando una particolare categoria di dati personali[492], possono essere altresì oggetto di abusi e discriminazioni se impiegati in modo deregolato.

Per tale ragione, sono state introdotte tre macro eccezioni (art. 5, 2-4) che prendono in considerazione la natura della situazione e le possibili conseguenze derivanti dal loro utilizzo[493]. Orbene, l'impiego sarebbe consentito per: i) trovare potenziali vittime di reato, compresi i minori scomparsi; ii) impedire minacce specifiche, sostanziali ed imminenti alla vita o all'incolumità personale (per es. un attacco terroristico); iii) individuare, localizzare, identificare o perseguire i

includere qualsiasi «*AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database data repository, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used*» (v. considerando n. 8). Cfr. COUNCIL OF THE EUROPEAN UNION, *Presidency compromise text*, 2021/0106(COD), 29.11.2021, reperibile all'indirizzo https://media-exp1.licdn.com/dms/document/C4D1FAQGuV1FL6qMDIA/feedshare-document-pdf-analyzed, (visualizzato in data 13.12.2021). Cfr. *supra* il capitolo II, § 2.1.1.

[489] Cfr. *supra* il § 1.3.

[490] Cfr. l'art. 5 par. 1, lett. *d*) e il considerando n. 33, allegato III(1) (a), 2021/0106(COD).

[491] Cfr. il considerando n. 18, 2021/0106(COD).

[492] Nel GDPR, i dati biometrici rientrano nelle categorie particolari di dati personali disciplinati nell'art. 9, il cui testo è reperibile all'indirizzo ùhttps://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016R0679 (visualizzato in data 25.8.2021).

[493] Cfr. l'art. 5 par. 1, lett. *d*), 2021/0106(COD).

soggetti sospettati di reato di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, come stabilito dalla legge di tale Stato membro[494]. Nel successivo paragrafo, si aggiunge che l'utilizzo dei sistemi *de quibus* dovrà inoltre essere ponderato sulla base della «natura della situazione» nonché sulle «conseguenze» che possono derivarne «per i diritti e le libertà di tutte le persone interessate», con particolare riguardo, nel primo caso, alla «gravità», alla «probabilità» ed all'«entità del danno causato dal mancato uso del sistema» (*a*) e, nella seconda ipotesi, alla «gravità», alla «probabilità» ed all'«entità» delle suddette conseguenze (*b*). Viene inoltre operato un riferimento esplicito alla necessità di stabilire limitazioni «temporali» e «geografiche», oltreché «personali», che siano «necessarie e proporzionate in relazione all'uso». In tutti questi casi, secondo la Commissione, l'impiego di questi strumenti sarebbe giustificato da ragioni rilevanti di pubblica sicurezza.

Per vero, emergono sin da una prima lettura alcuni dubbi interpretativi circa l'effettiva applicazione del regolamento in questi termini[495]. Quante volte, in occasione per esempio di grandi assembramenti, abbiamo avuto la sensazione di essere in presenza di una minaccia "sostanziale e imminente"? In quali occasioni potremmo essere sicuri di poter trovare una "potenziale vittima di reato", o un "bambino scomparso"? Oltre a questo, anche la terza eccezione potrebbe essere di complessa applicazione, dal momento che la gravità del reato, per permettere l'attivazione del sistema automatico, è valutata in base al massimo della pena edittale prevista per un determinato reato, che cambia anche per le stesse qualificazioni di reati nei vari Stati membri. Questo potrebbe portare a disparità di trattamento con conseguenti potenziali problematiche nell'ottica della cooperazione giudiziaria e di polizia. Infatti, potrebbe esserci il rischio che tale tipologia di strumento sia ammessa in uno Stato e non sia, per la stessa fattispecie di reato, attivabile in un altro Stato membro[496]. Oltretutto, la proposta lascia ai singoli ordinamenti la facoltà di decidere se attuare o meno le suddette eccezioni per l'impiego dei *tools* di

[494] Cfr. la decisione quadro del Consiglio 2002/584/GAI, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri (G.U. L. 190 del 18.7.2002, p. 1).

[495] In questo senso v. EDri, *EU's AI law needs major changes to prevent discrimination and mass surveillance*, 2021, reperibile all'indirizzo https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/ (visualizzato in data 20.1.2022).

[496] Inoltre, come è stato evidenziato, oltre «all'elenco delle fattispecie (…) – che in base al § 3 dello stesso art. 2 potrà essere integrato o modificato in qualsiasi momento con voto unanime del Consiglio europeo – (…)» che riguarda «un *genus* di crimini molto gravi e il cui *nomen iuris* attribuito nell'elenco è di adeguata determinatezza e di immediata percezione (così, «tratta di esseri umani», «sfruttamento sessuale dei bambini», «rapimento, sequestro e presa di ostaggi», ma anche «omicidio volontario» …)», sarebbero menzionati altresì «categorie assai larghe di infrazioni». In particolare, si prospetta il rischio che lo strumento di riconoscimento automatico possa essere attivato anche per fatti puniti con pene lievissime (o addirittura esenti da pena). Con riferimento al Mandato di arresto europeo cfr. M. Chiavario, *Diritto processuale penale*, IX° ed., Wolters Kluwer, Milano, 2022, p. 1294. Cfr. anche M. Hildebrandt, *The Proposal for an EU AI Act of 21 April 2021*, in *Brief Commentary*, 2021, reperibile all'indirizzo https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legalrequirements/F2662611_en (visualizzato in data 29.9.2021).

riconoscimento tramite specifiche leggi nazionali[497]. La Commissione, infatti, tiene conto del fatto che le questioni di sicurezza nazionale rimangono in ogni caso appannaggio esclusivo riservato agli Stati membri[498]. Oltre a ciò, la proposta di siffatto divieto generalizzato non includerebbe l'impiego di questi *tools* da parte di altre autorità (per esempio nelle scuole) ovvero da aziende private (per esempio supermercati, società di trasporti o stadi)[499].

V'è da aggiungere che l'utilizzo dei sistemi di riconoscimento automatici sarebbe soggetto in ogni caso ad un'espressa autorizzazione, da parte di un'autorità giudiziaria o di un'autorità amministrativa indipendente, emessa a seguito di richiesta motivata e nel rispetto delle suddette regole nazionali. Occorre accertare, pertanto, sulla base di «prove oggettive» o «indicazioni chiare», la necessità e la proporzionalità della misura rispetto ad almeno una delle finalità ammesse. L'unica ipotesi in cui risulta consentito prescindere dall'autorizzazione riguarda eventuali situazioni di urgenza, salva in ogni caso la necessità di ottenere la convalida (§ 3).

Con riferimento ai sistemi di riconoscimento impiegati in modalità "*post remote*", invece, la Commissione li classifica come "ad alto rischio", posto che «le inesattezze di carattere tecnico (…) possono determinare risultati distorti e comportare effetti discriminatori»[500].

L'impiego di questi sistemi non è vietato. Tuttavia, come già visto *supra*[501], è necessario che siano rispettati diversi requisiti obbligatori per garantire che tali *tools* «non presentino rischi inaccettabili

---

[497] Cfr. il considerando n. 22, 2021/0106(COD).

[498] Cfr. su questo punto T. Christakis, M. Becuywe, *Pre-Market Requirements, Prior Authorisation and Lex Specialis: Novelties and Logic in the Facial Recognition-Related Provisions of the Draft AI Regulation*, in *European Law Blog*, 2021, reperibile all'indirizzo https://europeanlawblog.eu/2021/05/04/pre-market-requirements-prior-authorisation-and-lex-specialis-novelties-and-logic-in-the-facial-recognition-related-provisions-of-the-draft-ai-regulation/ (visualizzato in data 20.1.2022) in cui gli Autori sostengono che l'art. 5 par. 1 lett. *d)* va interpretato come *lex specialis* in conformità a quanto stabilito dall'art. 10 LED (cfr. *supra* il § 4.1).

Il Consiglio dell'Unione europea ha di recente diffuso un primo testo di modifica delle disposizioni contenute nella proposta di regolamento della Commissione europea (COUNCIL OF THE EUROPEAN UNION, *Presidency compromise text*, 2021/0106(COD), 29.11.2021, reperibile all'indirizzo https://media-exp1.licdn.com/dms/document/C4D1FAQGuV1FL6qMDIA/feedshare-document-pdf-analyzed, visualizzato in data 13.12.2021) in cui ha ribadito la competenza esclusiva degli Stati membri in materia di sicurezza nazionale e ha insistito sul fatto che i sistemi di intelligenza artificiale sviluppati esclusivamente per scopi militari dovrebbero essere esclusi dal campo di applicazione del regolamento

[499] Si ricorda che il Consiglio dell'Unione europea nel primo testo di modifica delle disposizioni contenute nella Proposta diffuso di recente, ha aggiunto nell'art. 5 par. 1 lett. *d*) il riferimento ad altri soggetti che agiscono per conto delle autorità di contrasto o collaborano con esse, estendendo in tal modo a costoro il divieto d'impiego dei sistemi di riconoscimento "in tempo reale" in spazi aperti al pubblico. Inoltre, il Consiglio dell'Unione europea ha proposto che ognuna delle tre eccezioni sia descritta in modo più esaustivo e restrittivo, tenendo conto di alcuni elementi come, per esempio, la natura della situazione che ha dato origine alla richiesta, le conseguenze dell'uso per i diritti e le libertà di tutte le persone interessate e le garanzie e le condizioni previste per il suo utilizzo. Cfr. COUNCIL OF THE EUROPEAN UNION, *Presidency compromise text*, 2021/0106(COD), 29.11.2021, reperibile all'indirizzo https://media-exp1.licdn.com/dms/document/C4D1FAQGuV1FL6qMDIA/feedshare-document-pdf-analyzed, visualizzato in data 13.12.2021). Su questo punto v. M. Hildebrandt, The Proposal for an EU AI Act of 21 April 2021, *Brief Commentary*, 2021, cit.

[500] Cfr. il considerando n. 33, 2021/0106(COD).

[501] Cfr. il capitolo II, § 2.1.1.

per interessi pubblici importanti dell'Unione, come riconosciuti e tutelati dal diritto dell'Unione»[502]. Una volta che il sistema abbia ottenuto la certificazione di conformità ai requisiti suddetti, esso potrebbe essere immesso sul mercato, fermo restando che «qualsiasi trattamento di dati biometrici e di altri dati personali interessati dall'uso di sistemi di IA a fini di identificazione biometrica, diverso da quello connesso all'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto disciplinato dal presente regolamento, (…), dovrebbe continuare a soddisfare tutti i requisiti derivanti dall'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, dall'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725 e dall'articolo 10 della direttiva (UE) 2016/680»[503]. Oltre a ciò, la proposta prevede altresì l'introduzione di un sistema di verifica periodica di tali strumenti, eseguita da autorità nazionali competenti designate dagli Stati membri[504]. Giova ribadire che, a fronte della predisposizione di una serie di requisiti tecnici anche molto dettagliati ai quali gli *automated facial recognition systems* devono risultare conformi, la proposta non introduce analoghi strumenti sanzionatori per sanzionare eventuali trasgressioni. Il rischio che si corre è quello di considerare un sistema di autovalutazione tecnico eseguito dai fornitori di IA come una garanzia effettiva contro i pericoli che tali tecnologie possono generare per i diritti fondamentali[505].

Quanto ai sistemi di categorizzazione biometrica, che potrebbero essere ricondotti ragionevolmente nella macro categoria dei sistemi di riconoscimento facciale, sono stati definiti come quei *tools* di IA che impiegano i dati biometrici di persone fisiche «al fine di assegnarle a categorie specifiche, quali quelle basate sul sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, l'origine etnica o l'orientamento sessuale o politico»[506]. Non essendo classificati come sistemi "ad alto rischio", essi sarebbero soggetti solamente alle regole di trasparenza concernenti le informazioni da fornire alle persone fisiche che sono esposte sul funzionamento del sistema. Tale proposta di classificazione appare, anche sotto questo punto di vista, piuttosto discutibile[507]. Infatti, la distinzione fra sistema impiegato a fini di categorizzazione e a fini di riconoscimento rischia di diventare una *quaestio* puramente arbitraria. L'impiego in spazi aperti al pubblico di sistemi di categorizzazione biometrica[508]

[502] Cfr. il considerando n. 27, 2021/0106(COD). Si rimanda al capitolo II, § 2.1.1. per l'approfondimento dei requisiti predisposti dalla Commissione europea.
[503] Cfr. il considerando n. 24, 2021/0106(COD).
[504] Cfr. l'art. 61, 2021/0106(COD).
[505] Cfr. il capitolo II, § 2.1.1.
[506] Cfr. l'art. 3 par. 35, 2021/0106(COD).
[507] Su questo punto v. M. Ebers, V.R.S. Hoch, F. Rosenkranz, H. Ruschemeier, B. Steinrötter, *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society*, in (RAILS). J. 2021, 4(4), pp. 589-603 e M. Hildebrandt, *The Proposal for an EU AI Act of 21 April 2021*, in *Brief Commentary*, 2021, cit.
[508] Cfr. *supra* il § 1.

potrebbe avere un impatto altrettanto negativo sui diritti fondamentali degli individui[509]. A titolo esemplificativo, è stato evidenziato come questi sistemi potrebbero essere utilizzati dalle autorità di polizia per «*classifying people in public places as of a certain ethnicity or political orientation*», posto che «*they are under no obligation to include human oversight, or to notify people that the system is in use*»[510]. A tal proposito, l'*European Data Protection Supervisor* (EDPS) sostiene che si dovrebbe adottare un approccio più rigoroso per la regolamentazione dell'impiego del riconoscimento automatizzato in spazi aperti al pubblico, indipendentemente che questi siano utilizzati in un contesto commerciale, amministrativo o di *law enforcement*[511]. Infatti l'EDPS, insieme all'*European Data Protection Board* (EDPB), in un parere congiunto non vincolante hanno proposto un «*general ban on any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals - in any context*»[512], dal momento che «*problem regarding the way to properly inform individuals about this processing is still unsolved*»[513]. Oltre a ciò, «*the intrusiveness of the processing does not always depend on the identification being done in real-time or not. Post remote biometric identification in the context of a political protest is likely to have a significant chilling effect on the exercise of the fundamental rights and freedoms, such as freedom of assembly and association and more in general the founding principles of democracy. Second, the intrusiveness of the processing does not necessarily depend on its purpose. The use of this system for other purposes such as private security represents the same threats to the fundamental rights of respect for private and family life and protection of personal data*»[514].

In conclusione, la proposta costituisce certamente un buon punto di partenza. Vi sono però alcune criticità che potrebbero emergere in fase applicativa qualora il testo normativo non dovesse subire modifiche o integrazioni[515]. Come evidenziato, sarà interessante comprendere come le diverse

[509] Cfr. sul punto G. Malgieri and M. Ienca, *The EU regulates AI but forgets to protect our mind*, 7.7.2021, reperibile all'indirizzo https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/ (visualizzato in data 20.1.2022).

[510] Cfr. C. Kind, Containing the canary in the AI coalmine – the EU's efforts to regulate biometrics, *Ada Lovelace Institute*, 2021, reperibile all'indirizzo https://www.adalovelaceinstitute.org/blog/canary-ai-coalmine-eu-regulate-biometrics/ (visualizzato in data 20.1.2022).

[511] Cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary*, 2021, reperibile all'indirizzo https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en (visualizzato in data 20.1.2022).

[512] Cfr. EDPB – EDPS, *Joint opinion 5/2021*, 18.6.2021, p. 3, reperibile all'indirizzo https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf (visualizzato in data 20.1.2022).

[513] Cfr. EDPB – EDPS, *Joint opinion 5/2021*, 18.6.2021, cit., p. 12.

[514]Cfr. EDPB – EDPS, *Joint opinion 5/2021*, 18.6.2021, cit., p. 12.

[515] Si ritiene che difficilmente il testo rimarrà formulato in questi termini dal momento che, come anticipato *supra* (cfr. il § 4), in occasione della pubblicazione della Risoluzione 2020/2016(INI) - "*Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*", il Parlamento europeo ha votato per richiedere una moratoria sull'adozione di sistemi di riconoscimento facciale a fini identificativi, a meno che non siano usate strettamente ai fini dell'identificazione delle vittime di reati (§ 27), fino a quando non vi sarà una normativa di riferimento che attesti la conformità di tali sistemi ai diritti fondamentali

eccezioni al divieto del riconoscimento in modalità "*real time*" da parte delle autorità di *law enforcement* in spazi aperti al pubblico opereranno in concreto e come l'interpretazione del regolamento ne verrà di riflesso condizionata. In tal senso, l'Italia, con l'introduzione del d.l. 139/2021 (cd. "*decreto Capienze*") conv. con l. 205/2021, si è posta in netta antitesi rispetto all'approccio proposto dalla Commissione europea e, a questo punto, anche rispetto all'orientamento ormai consolidato della Corte di giustizia che, come ricordato più volte *supra*, a fronte di intrusioni significative nella sfera privata e dei dati personali degli individui, sostiene fermamente la necessità di introdurre specifiche «norme di legge, di modo che l'acquisizione per fini di prevenzione o di accertamento processuale sia circoscritta al ricorrere di reati sufficientemente gravi» e «contenuta nella misura strettamente necessaria per conseguire il fine perseguito», ma anche «accompagnata dal controllo preventivo di un giudice o di una entità amministrativa indipendente»[516].

5. Considerazioni conclusive

Con il presente capitolo, si sono analizzate più specificamente le *automated facial recognition technologies* alla luce della ricostruzione tecnico-giuridica, operata nei primi capitoli della presente ricerca, avente ad oggetto - più in generale - il rapporto fra le tecnologie di riconoscimento biometrico e il procedimento penale. La scelta di approfondire il riconoscimento facciale è stata dettata dall'enorme potenziale raggiunto negli ultimi anni da questa tecnologia. L'impiego di software automatici di riconoscimento facciale non richiede alcuna collaborazione da parte del soggetto passivo e il sistema non risulta assoggettabile ad alcun cambiamento comportamentale, volontario o meno, da parte dell'individuo sottoposto a riconoscimento. Per tale ragione, tali tecnologie sono state integrate in diversi dispositivi, come sistemi di telecamere a circuito chiuso o *smartphone*, rendendo sempre più agevole la raccolta e la comparazione delle immagini ivi registrate, per il perseguimento delle finalità più varie. Entro tale contesto, in Italia s'inserisce - dal 2017 - l'impiego, da parte degli organi di polizia, del "Sistema Automatico Riconoscimento Immagini" conosciuto ai più con la sigla del suo acronimo "S.A.R.I.". L'utilizzo di tale strumento costituisce certamente un vantaggio, sia sul piano della velocità sia su quello dell'efficienza. L'impiego del software rientrerebbe nel vasto filone di tecniche inedite che l'inarrestabile sviluppo scientifico degli ultimi anni ha prodotto e di cui fanno parte diversi strumenti, entro dunque l'ampia categoria delle "indagini atipiche". S.A.R.I. *Enterprise*

e vi saranno prove empiriche della necessità e della proporzionalità per la diffusione dell'impiego di tali tecnologie. Sulla base di questo documento, è possibile immaginare quali saranno le argomentazioni del Parlamento europeo durante la votazione della proposta di regolamento sull'Intelligenza artificiale.

[516] T. Rafaraci, *Verso una law of evidence dei dati*, in *Dir. pen. proc.*, 2021, p. 853. Cfr. *supra* il capitolo I, § 1.1.

risulta ad oggi impiegato dalla polizia giudiziaria per eseguire solamente una prima macro ricerca nel database A.F.I.S.-S.S.A. fra i soggetti precedentemente foto segnalati: il risultato scaturente dal software agevola così una prima scrematura fra più possibili direzioni di indagine.

Dal punto di vista probatorio, si sono eseguite poi le consuete distinzioni aventi ad oggetto la diversa natura delle rappresentazioni digitalizzate dei tratti coinvolti in una data comparazione automatica tramite software. Quanto al *match* scaturente da sistemi automatici di riconoscimento impiegati comparando le *features* ricavate da un'immagine digitale attraverso procedimenti di digitalizzazione, si è visto che il controllo sul risultato spetta sempre ad un tecnico che applicherà una metodologia di comparazione forense manuale. In questo modo, il giudice valuterà direttamente la prova presentata dall'operatore specializzato. Con riferimento invece al *match* o *non match* generato automaticamente da un dispositivo IoT ad uso generico/commerciale, seppur il canale d'ingresso possa essere rappresentato dall'art. 189 c.p.p., sono emerse diverse criticità circa il vaglio da compiersi sulla sua concreta ammissibilità, tenendo conto dei requisiti richiesti dalla norma, anche alla luce della più consolidata giurisprudenza. Con riferimento alla modalità in "*Real time*" del software S.A.R.I., si è prospettato, infine, un loro possibile accostamento alla disciplina di matrice giurisprudenziale delle videoregistrazioni, quanto meno come punto di partenza per una possibile futura regolamentazione.

Si sono poi passate in rassegna alcune delle libertà e garanzie fondamentali su cui le tecniche di riconoscimento facciale risultano potenzialmente in grado di incidere, analizzando due recenti sentenze d'oltremanica aventi ad oggetto la modalità in "*real time*" dei software di riconoscimento facciale impiegati dalle autorità di polizia in contesti pubblici. Rivendicare una dimensione digitale del garantismo penale obbliga a interrogarsi sulla ragionevolezza del sacrificio imposto alle garanzie processuali fondamentali dell'individuo da strumenti di indagine come i software di riconoscimento facciale. Più nel dettaglio, dal delineato quadro normativo sovranazionale è emersa la pressoché unanime intenzione, sia nell'ambito dell'Unione europea sia in quello del Consiglio d'Europa, di promuovere l'eccellenza nell'IA e le sue applicazioni virtuose, nel rispetto però dei diritti fondamentali dell'individuo. In generale, la preoccupazione maggiore rilevata nell'ambito dell'impiego di tali tecnologie è rappresentata proprio dalla mancanza di una disciplina normativa di riferimento e dai potenziali rischi correlati all'impiego di strumenti di tal genere. Neppure la proposta di regolamento sull'intelligenza artificiale da parte della Commissione europea è riuscita a spazzare via i timori e le preoccupazioni per i diritti e le libertà fondamentali. Il dibattito sull'applicazione delle tecnologie di riconoscimento facciale nel processo penale sembra ormai giunto ad una fase avanzata, in cui non è più in discussione l'*an,* bensì il *quomodo* di regolamentazione di questi sistemi. È evidente come tutti gli argomenti qui brevemente richiamati rappresentino solo alcune riflessioni per un ragionamento futuro che dovrà raggiungere gli aspetti più essenziali dei sistemi di giustizia europei.

Ciò sollecita un costante dibattito scientifico e la costruzione di un glossario comune e multidisciplinare che presti la massima attenzione agli strumenti che ormai da tempo sono penetrati nei nostri ordinamenti.

CONCLUSIONI

Sembra si possa affermare, in via definitiva, che – sia a livello domestico, sia nel contesto sovranazionale – vi sia una decisa tendenza verso l'introduzione di una disciplina normativa specifica che sia in grado di valorizzare le diverse peculiarità tecniche degli *automated biometric recognition systems* impiegati per finalità di *law enforcement*. Ciascuno strumento in grado di estrarre, analizzare e comparare diversi dati fisici, fisiologici o comportamentali deve godere ormai di una regolamentazione a sé. A tal proposito, ci si è interrogati circa l'effettiva funzione informazionale di un *match* o un *non-match* scaturente da uno strumento automatizzato e il suo specifico contributo conoscitivo rispetto al *thema probandum* nel procedimento penale. Sono state presentate alcune brevi riflessioni sull'attendibilità di corrispondenza fra due rappresentazioni digitalizzate di dati biometrici ovvero dei relativi *templates*, introducendo il parametro del calcolo del rapporto di verosimiglianza rispetto ad una data popolazione di riferimento. Da ciò, poste le dovute distinzioni, si sono prospettati alcuni dubbi interpretativi rispetto alla concreta possibilità di valutare il requisito dell'idoneità dello strumento probatorio considerato nell'assicurare l'accertamento del fatto, alla luce della ormai consolidata interpretazione giurisprudenziale in tema di "nuova prova scientifica". Il giudice dovrà sempre ragionare caso per caso, tenendo in considerazione la natura dello specifico tratto biometrico considerato, il contesto di acquisizione del dato, la metodologia impiegata nel trattamento, il software utilizzato e la descrizione degli algoritmi alla base dello stesso.

L'adozione di questi strumenti, poi, deve essere consentita purché munita di specifiche garanzie. O meglio, il regime normativo ragionevolmente differenziato dovrà tenere conto di diversi fattori da cui dipende il maggiore o il minore grado di "invadenza". Anche la normativa per la protezione del trattamento dei dati personali da parte delle autorità, a fini di prevenzione, investigazione e repressione dei reati, rispetto all'impiego di taluni strumenti automatizzati, ha sollevato alcuni dubbi esegetici circa la conformità di alcune modalità applicative di questi *tools*. Il punto di partenza sembra, infatti, essere rappresentato dalla ormai diffusa consapevolezza dell'estrema insidiosità di alcune tecniche inedite di riconoscimento, i cui risultati potrebbero altresì giungere – come visto – nella successiva fase dibattimentale. A causa del consueto ritardo strutturale del diritto rispetto al progredire della scienza e della tecnica, si ritiene fisiologico che la genesi e l'applicazione di nuovi *automated biometric tools* siano avvenuti entro un contesto di vuoto normativo. Com'è noto, la disciplina giuridica ha anche il compito di intervenire a posteriori

per risolvere problematiche preesistenti e rendere compatibili determinati impieghi delle tecnologie con i diritti fondamentali. In attesa di un intervento legislativo, la giurisprudenza ha solitamente svolto un ruolo di supplenza, nell'intento di realizzare un equo bilanciamento tra le esigenze di accertamento penale e le istanze di tutela dei diritti inviolabili, sempre più messi a rischio dal progresso tecnologico. Tuttavia, come si è visto, le pronunce delle Corti chiamate ad interrogarsi sul regime giuridico concretamente applicabile ad alcuni strumenti di riconoscimento, e a delimitarne i confini applicativi, si sono mostrate incerte, defilate e, a tratti, non hanno dimostrato la necessaria elasticità ermeneutica nel cogliere l'attuale cambiamento di paradigma. L'affiorare di alcune pronunce giurisprudenziali d'oltremanica in tema di impiego di *automated facial recognition systems*, infatti, ha dato luogo a notevoli incertezze e discussioni che sono specchio della confusione politico-normativo attuale, quest'ultima peraltro altresì presente nell'ambito della cooperazione giudiziaria internazionale per lo scambio di questa particolare categoria di dati personali. Anche sul versante dottrinale, già a partire dalle più semplici *quaestiones* definitorie, non si sono ad oggi formati orientamenti consolidati, forse perché l'impiego di taluni strumenti di riconoscimento pone ancora al giurista questioni epistemologiche troppo complesse. Ecco allora sorgere l'esigenza di costruire un glossario comune tra le diverse discipline sotto l'egida di un ormai avviato dibattito scientifico e multidisciplinare su strumenti che da tempo sono penetrati nei nostri ordinamenti. A tal proposito, sono emersi "diversi livelli di complessità" che il dato biometrico *tout court* pone, considerata l'intrinseca specificità delle fonti di prova in esame. La disciplina biometrica applica principi e si serve di misurazioni che attingono alle più differenti discipline: dalla biologia alla statistica, dalla fisica all'informatica. Entro tale contesto, il procedimento di identificazione, autenticazione o categorizzazione di un individuo, è stato oltremodo agevolato dall'impiego di processi automatizzati, i quali consentono di estrarre automaticamente caratteristiche fisiche, fisionomiche o comportamentali non direttamente visibili, rendendo agevoli confronti e valutazioni metriche. Tuttavia, molto più di quanto sia possibile osservare nel territorio nazionale, a livello mondiale l'applicazione di tecniche di intelligenza artificiale al riconoscimento automatico in un contesto di *law enforcement* costituisce – oggi più che mai – in termini di completezza, attendibilità e compatibilità del risultato con le tradizionali garanzie processuali, un tema estremamente dibattuto. Particolarmente significativi, in tal senso, sono stati i recenti documenti normativi sovranazionali che hanno mostrato un impegno significativo per l'individuazione e la riduzione al minimo dei rischi connessi all'impiego di tali mezzi di riconoscimento. Proprio le più recenti proposte legislative eurounitarie rendono però opportune alcune precisazioni finali. È bene infatti rammentare che i

criteri proposti a livello sovranazionale costituiscono sì un valido punto di partenza comune, da cui attingere e prendere l'abbrivio; tuttavia, come si è visto, non paiono ancora sufficienti né quantitativamente, né qualitativamente, per sostenere, da soli, il peso di rappresentare la normativa di riferimento per i regimi nazionali in materia di *automated biometric recognition systems*. La recente proposta di regolamento sull'intelligenza artificiale, al fine di proteggere i diritti e le garanzie fondamentali, contiene numerose prescrizioni tecniche da rispettare senza stabilire concretamente gli effetti e i rimedi di eventuali trasgressioni. Peraltro, l'Italia, rispetto al più specifico settore degli *automated facial recognition systems*, con l'introduzione del d.l. 139/2021 (cd. "*decreto Capienze*") conv. con l. 205/2021, si è posta in netta antitesi rispetto all'approccio proposto dalla Commissione europea, non dimostrando piena consapevolezza dei diversi livelli di complessità coinvolti in questa materia e dei rischi in gioco per i diritti e le libertà fondamentali dell'individuo.

La futura regolamentazione dovrà tenere certamente in considerazione diversi fattori. In primo luogo, le previsioni normative da introdurre dovranno essere il più possibile "neutrali" da un punto di vista tecnico-scientifico, al fine di evitare una rapida obsolescenza delle stesse. Dovrà essere presa in considerazione ciascuna potenziale violazione o intrusione nelle garanzie processuali e libertà fondamentali dell'individuo con l'introduzione di un controllo giurisdizionale e dei concreti rimedi contro eventuali trasgressioni, evitando di lasciare agli organi inquirenti completa discrezionalità anche nei casi di maggiore urgenza. Infine, si ritiene quanto mai necessaria la messa a punto di una più specifica "*biometric chain of custody*" che tenga conto delle specifiche tecniche di ciascun sistema di riconoscimento impiegato a fini giudiziari. È tempo di intervenire con un approccio rigoroso e consapevole dei fondamenti e dei limiti di questi peculiari strumenti automatici di riconoscimento, cogliendo le sorprendenti opportunità del progresso scientifico nel campo investigativo e prevenendo i rischi per le garanzie processuali correlati al loro impiego.

BIBLIOGRAFIA

AA.VV. *La prova scientifica nel processo penale*, (a cura di) L. De Cataldo Neuburger, Cedam, Padova, 2007;

AA.VV. *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Luparia, Cedam, Milano;

AA.VV., *AI and Deep Learning in Biometric Security*, (a cura di) G. Jaswal, V. Kanhangad, R. Ramachandra, CRC Press, Boca Raton, 2021;

AA.VV., *Algorithmic Governance and Governance of Algorithms, Legal and Ethical Challenges*, (a cura di) M. Ebers, M. Cantero Gamito, Springer, Berlin, 2020;

AA.VV., *Algorithms and Law*, (a cura di) M. Ebers, S. Navas Navarro, Cambridge University Press, Cambridge, 2020;

AA.VV., *Banca dati del DNA e accertamento penale*, (a cura di) L. Marafioti, L. Luparia, Giuffrè, Milano, 2010;

AA.VV., *Carta dei diritti fondamentali dell'Unione europea*, (a cura di) R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini, Giuffrè, Milano, 2017;

AA.VV., *Commentario alla Costituzione. Principi fondamentali*, (a cura di) G. Branca, Zanichelli, Bologna, 1975;

AA.VV., *Commento al nuovo codice di procedura penale*, (a cura di) M. Chiavario, Utet, Torino, II, 1990;

AA.VV., *Commento al nuovo codice di procedura penale*, (a cura di) M. Chiavario, Utet, Torino, 1991;

AA.VV., *Compendio di Procedura Penale*, (a cura di) G. Conso, V. Grevi, M. Bargis, Cedam, Padova, 2014;

AA.VV., Computer forensics *e Indagini digitali*, (a cura di) S.Aterno, F.Cajani, G.Costabile, M.Mattiucci, G.Mazzarco, Experta, Forlì, 2011;

AA.VV., *Contrasto al terrorismo interno e internazionale*, (a cura di) R.E. Kostoris, R. Orlandi, Giappichelli, Torino, 2006;

AA.VV., *Cooperazione informativa e giustizia penale nell'Unione europea*, (a cura di) F. Peroni, M. Gialuz, EUT - Edizioni Università di Trieste, Trieste, 2009;

AA.VV., *Crime, Procedure and Evidence in a Comparative and International Context. Essays in Honour of Professor Mirijan Damaŝka*, (a cura di) J. Jakcson, M. Langer, P. Tillers, Hart Publishing, Oxford-Portland, 2008;

AA.VV., Cyber forensics *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, (a cura di) S. Aterno, F. Cajani, G. Costabile, D. Curtotti, Giappichelli, Torino, 2021;

AA.VV., *Cybercrime, Trattati giuridici Omnia*, (a cura di) A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Utet giuridica, Milano, 2019;

AA.VV., *Decisione robotica*, (a cura di) A. Carleo, Il Mulino, Bologna, 2019;

AA.VV., *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations*, (a cura di) M. Caianiello, A. Camon, Wolters Kluwer, Milano, 2021;

AA.VV., *Diritti della persona e nuove sfide del processo penale*, (a cura di) L. Kalb, Giuffrè, Milano, 2019;

AA.VV., *Diritti e libertà in internet*, (a cura di) O. Pollicino, T.E. Frosini, E. Apa, Mondadori, Milano, 2017;

AA.VV., *Diritto e intelligenza artificiale*, (a cura di) G. Alpa, Pacini eds., Pisa, 2020;

AA.VV., *Etica e diritto. Le vie della giustificazione razionale*, (a cura di) L. Gianformaggio, E. Lecaldano, Bari, 1986;

AA.VV., *EU Law in Populist Times*, (a cura di) F. Bignami, Cambridge University Press, Cambridge, 2020;

AA.VV., *Face recognition: methods, applications and technology*, (a cura di) A. Quaglia, C. M. Epifano, NOVA Publishers, Enschede, 2010;

AA.VV., *GDPR e normativa privacy. Commentario*, (a cura di) G.M. Riccio, G. Scorza, E. Belisario, 1a ed., Giuffrè, Milano, 2018;

AA.VV., *Genetica forense e diritto: prospettive scientifiche, tecnologiche e normative*, (a cura di) M. Dobosz, E. Carnevali, M. Lancia, Giuffrè, Milano, 2011;

AA.VV., *Giurisprudenza sistematica di diritto processuale penale*, (dir. da) M. Chiavario, E. Marzaduri, Giappichelli, Torino, 1999;

AA.VV., *Giusto processo. Nuove norme sulla formazione e valutazione della prova* (l. 1° marzo 2001, n. 63), (a cura di) P. Tonini, Cedam, Padova, 2001;

AA.VV., *Global Law. Legal Answers for Concrete Challenges*, (a cura di) M.L. Labate Mantovanini Padua Lima, J. Garcez Ghirardi, Juruà Editorial, Porto, 2018;

AA.VV., *Handbook of Biometrics for Forensic*, (a cura di) M. Tistarelli, C. Champod, Springer, Cham, 2017;

AA.VV., *Human Rights in European Criminal Law. New Developments in European Legislation and Case Law after the Lisbon Treaty*, (a cura di) S. Ruggeri, Springer, Cham, 2015;

AA.VV., *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, (a cura di) L. Scaffardi, Giappichelli, Torino, 2018;

AA.VV., *I saperi del giudice. La causalità e il ragionevole dubbio*, (a cura di) F. Stella, Giuffrè, Milano, 2004;

AA.VV., *Il codice dei dati personali. Temi e problemi*, (a cura di) F. Cardarelli, S. Sica, V. Z. Zencovich, Giuffrè Editore, Milano, 2004;

AA.VV., *Il concetto di prova alla luce dell'intelligenza artificiale*, (a cura di) J. Sallantin, J.J. Szczeciniarz, Giuffrè, Milano, 2005;

AA.VV., *Il diritto penale dell'informatica*, (a cura di) L. Picotti, Cedam, Padova, 2004;

AA.VV., *Il processo penale accusatorio*, (a cura di) E. Stefani, Giuffrè, Milano, 2013;

AA.VV., *Indagini penali e amministrative in materia di frodi IVA e doganali. L'impatto dell'European Investigation Order sulla cooperazione transnazionale*, (a cura di) A. Di Pietro, M. Caianiello, Cacucci, Bari, 2016;

AA.VV., *Intelligenza artificiale, protezione dati personali e regolazione*, (a cura di) F. Pizzetti, Giappichelli, Torino, 2018;

AA.VV., *Intelligenza artificiale. Algoritmi giuridici Ius condendum o "fantadiritto"?*, (a cura di) G. Taddei Elmi, A. Contaldo, Pacini editore, Pisa, 2020;

AA.VV., *Investigazioni digitali*, (a cura di) M. Iaselli, Giuffrè, Milano, 2020;

AA.VV., *L'uso della prova scientifica nel processo penale*, (a cura di) M. Cucci, G. Gennari, A. Gentilomo, Maggioli, Santarcangelo di Romagna, 2012;

AA.VV., *La Banca dati italiana del Dna. Limiti e prospettive della genetica forense*, (a cura di) L. Scaffardi, Il Mulino, Bologna, 2019;

AA.VV., *La conoscenza del fatto nel processo penale*, (a cura di) G. Ubertis, Giuffrè, Milano, 1992;

AA.VV., *La libertà personale dell'imputato. Verso il nuovo processo penale*, (a cura di) V. Grevi, Cedam, Padova, 1989;

AA.VV., *La nuova disciplina europea della privacy*, (a cura di) S. Sica, V. D'Antonio, G. M. Riccio, Giuffrè, Milano, 2016;

AA.VV., *La prova nel dibattimento penale*, (a cura di) P. Ferrua, F. M. Grifantini, Giappichelli, Torino, 2007;

AA.VV., *La prova penale*, (a cura di) A. Gaito, Utet, Torino, 2008;

AA.VV., *La prova scientifica nel processo penale*, (a cura di) L. De Cataldo Neuburger, Cedam, Padova, 2007;

AA.VV., *La prova scientifica nel processo penale*, (a cura di) Tonini P., supplemento a *Dir. pen. proc.*, n. 6, 2008, p 52;

AA.VV., *La prova tecnica nel processo penale. Aspetto pratico scientifici*, (a cura di) A. Barbaro, A. La Marca, E. Nobile, P. Romeo, Editore Key, Firenze, 2016;

AA.VV., *Le nuove intercettazioni*, (a cura di) O. Mazza, Giappichelli, Torino, 2018;

AA.VV., *Le nuove norme di contrasto al terrorismo*, (a cura di) A. A. Dalia, Giuffrè, Milano, 2006;

AA.VV., *Le nuove norme sulla sicurezza pubblica*, (a cura di) S. Lorusso, Cedam, Padova, 2008;

AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, e scienze*, (a cura di) D. Curtotti, L. Saravo, Giappichelli, Torino, 2019;

AA.VV., *Manuale di informatica giuridica e diritto delle nuove tecnologie*, (a cura di) M. Durante, U. Pagallo, Utet, Torino, 2012;

AA.VV., *Media Technologies*, (a cura di) T. Gillespie, P. Boczkowki, K. Foot, Cambridge US, 2014;

AA.VV., *Novità su impugnazioni penali e regole di giudizio*, (a cura di) A. Scalfati, Ipsoa, Milano, 2006;

AA.VV., *Nuove norme in materia di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, (a cura di) G. Giostra, R. Orlandi, Giappichelli, Torino, 2018;

AA.VV., *Pattern Recognition. ICPR International Workshops and Challenges*, (a cura di) A. Del Bimbo, ICPR 2021, vol 12663, Springer, Cham;

AA.VV., *Pre-investigazioni (Espedienti e mezzi)*, (a cura di) A. Scalfati, Giappichelli, Torino, 2020;

AA.VV., *Prelievo del Dna e banca dati nazionale*, (a cura di) A. Scarcella, Cedam, Milano, 2009;

AA.VV., *Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology*, (a cura di) M. Hildebrandt, K. De Vries, Routledge, Abingdon, 2013;

AA.VV., *Privacy, Security and Accountability. Ethics, Law and Policy*, (a cura di) A.D. Moore, Rowman & Littlefield, New York, 2016;

AA.VV., *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, (a cura di) D. Negri, Aracne, Roma, 2007;

AA.VV., *Prova penale e metodo scientifico*, (a cura di) S. Lorusso, Utet, Torino, 2009;

AA.VV., *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Luparia, Cedam, Padova, 2018;

AA.VV., *Questioni di informatica forense*, (a cura di) C. Maioli, Aracne, Roma, 2015;

AA.VV., *Regulating Biometrics: Global Approaches and Urgent Questions*, (a cura di) A. Kak, AI Now Institute, 2020;

AA.VV., *Research Hanbook on the Law of Artificial Intelligence*, (a cura di) W. Barfield, U. Pagallo, Edward Elgar publishing, Cheltenham-Northampton, 2018;

AA.VV., *Scienza e causalità*, (a cura di) S. Seminara, C. De Maglie, Cedam, Padova, 2006;

AA.VV., *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, (a cura di) C. Conti, Giuffrè, Milano, 2011;

AA.VV., *Scienze forensi. Teoria e prassi dell'investigazione scientifica*, (a cura di) M. Picozzi, A. Intini, Utet, Torino, 2009;

AA.VV., *Semantica e filosofia del linguaggio*, Giuffrè, Milano, 1969;

AA.VV., *Sistema penale e criminalità informatica*, (a cura di) L. Luparia, Giuffrè, Milano, 2009;

AA.VV., *Studi di diritto processuale penale*, (a cura di) G. Conso, Giuffrè, Milano, 1980;

AA.VV., *Studio sul processo penale in ricordo di Assunta Mazzarra*, (a cura di) A. Gaito, Padova, Cedam, 1996;

AA.VV., *The Fight Against Impunity in EU Law*, (a cura di) L. Marin e S. Montaldo, Hart Publishing, New York, 2020;

AA.VV., *The Handbook of Face Recognition*, (a cura di) Z.S. Li, A.K. Jain, Springer, New York, 2011;

AA.VV., *Trattato di biodiritto*, vol. I, (a cura di) S. Rodotà – M. Tallachini, Giuffrè, Milano, 2011;

AA.VV., *Trattato di procedura penale*, (diretto da), G. Spangher, Utet giuridica, Torino, 2011;

AA.VV., *Sistema penale e criminalità informatica*, (a cura di) L. Lupària, Giuffrè, Milano, 2009;

ADINI Y., MOSES Y., ULLMAN S., *Face recognition: The Problem of Compensating for Changes, in Illumination Direction,* in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, v. 19 no. 7 (July 1997), 721–732;

ADORNO R., *Il prelievo a fini investigativi*, in *Giur. it*., 2010, III, p. 1238;

AGOSTINIS S., CATENACCI B., *Crimini e scrittura. La perizia grafica negli Stati Uniti*, Aras, Pesaro-Urbino, 2012;

AGOSTINO L., PERALDO M., *Le intercettazioni con captatore informatico: ambito di applicazione e garanzie procedurali*, in *Diritto di Internet, digital copyright and data protection*, suppl. fasc. 3/2020;

AITKEN C., TARONI F., *Statistics and the Evaluation of Evidence for Forensic Scientists*, Wiley, New York, 2004;

AITKEN C., ROBERTS R., JACKSON G., *Fundamentals of probability and statistical evidence in criminal proceedings: guidance for judges, lawyers, forensic scientists and expert witnesses*, Royal Statistical Society, London, 2010;

ALBANO LEONI F., MATURI P., *Fonetica sperimentale e fonetica giudiziaria*, in *Giur. it*., 1991, I, p. 316;

ALBERINI L., *Sul documento informatico e sulla firma digitale (novità legislative)*, in *Giust. civ*., 1998;

ALESCI T., *Il corpo umano fonte di prova*, Wolters Kluwer, Milano, 2017;

ALLEN R. J., KUHNS B. R., SWIFT E., *Evidence. Text, problems and cases*, Wolters Kluver, New York, 2012;

AMATO A., FLORA G., VALBONESI C., *Scienza, diritto e processo penale nell'era del rischio*, Giappichelli, Torino, 2019;

AMATO G., *Commento all'art. 13 Cost*., in AA.VV., *Commentario alla Costituzione*, (a cura di) G. Branca, Zanichelli, Bologna, 1977;

AMATO MANGIAMELI A.C., *Algoritmi e big data. Dalla carta sulla robotica*, in *Rivista di filosofia del diritto*, 1, 2019, 107 ss.;

AMATO S., CRISTOFARI F., RACITI S., *Biometria-I codici a barre del corpo*, Giappichelli, Torino, 2013;

AMODIO E., *Libertà e legalità della prova nella disciplina della testimonianza*, in *Riv. it. dir. proc. pen.*, 1973;

AMODIO E., *Giusto processo, procès équitable e fair trial: la riscoperta del giusnaturalismo processuale in Europa*, in *Riv. it. dir. e proc. pen.*, fasc.1-2, 2003, p. 93;

AMODIO E., *Il dibattimento nel nuovo rito accusatorio*, in *Giust. pen*., 1989, III, c. 580;

AMODIO E., *Perizia e consulenza tecnica nel quadro probatorio del nuovo processo penale*, in *Cass. pen*., 1989;

AMODIO E., *Processo penale, diritto europeo e common law*, Giuffrè, Milano, 2003;

AMODIO E., O. DOMINIONI, *Commentario del nuovo codice di procedura penale*, vol. I, Giuffrè, Milano, 1989, p. XXXVII;

ANCHETA A. N., *Scientific evidence and equal protection of the law*, Rutgers University Press, New Jersey, 2006;

ANDREOLI A., *Identità alla prova. La controversa storia del test del Dna tra crimini, misteri e battaglie legali*, Sironi, Milano, 2009;

ANDRIOLI V., *Diritto processuale civile I*, Jovene, Napoli, 1979;

ANGELETTI R., *Il processo indiziario. Indizio, sospetto e congettura al vaglio della giurisprudenza di legittimità*, Giappichelli, Torino, 2021;

APRILE E., *Le indagini tecnico-scientifiche: problematiche giuridiche sulla formazione della prova penale*, in *Cass. Pen*., 2003;

ARONSON D., *Genetic Witness. Science, Law and Controversy in the making of Dna profiling*, Rutgers University Press, New Brunswick, 2007;

ATERNO S., *Acquisizione e analisi della prova informatica*, in *Dir. pen. proc*., 2008, *Suppl. Dossier. La prova scientifica nel processo penale*;

ATERNO S., *Le investigazioni informatiche e l'acquisizione della prova digitale*, *Giur. merito*, fasc.4, 2013, p. 0955B;

AWAD A.I., HASSANIEN A.E., *Impact of Some Biometric Modalities on Forensic Science*, in AA.VV., *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications*, (a cura di) A.K. Muda et al., in *Studies in Computational Intelligence* 555;

BACCARI G.M., CONTI C., *La corsa tecnologica tra costituzione, codice di rito e norme sulla privacy: uno sguardo d'insieme*, in *Dir. Pen. e Processo*, 2021, 6, 711;

BACHOO A. K., TAPAMO J. R., *Texture Detection for Segmentation of Iris Images*, Proceedings of Saicsit, 2005, pp. 111–118, in http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.192.6766&rep=rep1&type=pdf ;

BALESTRA L., *La dichiarazione giudiziale di paternità e maternità alla luce della riforma della filiazione*, in *Rivista Trimestrale di Diritto e Procedura Civile*, fasc.4, 2014, p. 1223;

BALLERO B., *Tutela sostanziale del diritto di difesa e nuovo corso della giurisprudenza*, in *Giur. Cost*., 1972, p. 997;

BALOSSINO N., SIRACUSA S., *L'identificazione basata sul volto: metodi fisionomici e metrici*, disponibile in www.itasforum.it/pdf.phf?file=78_7%20-%20Balossino_Siracusa.pdf ;

BALSAMO A., KOSTORIS R.E., *Giurisprudenza europea e processo penale italiano*, Giappichelli, Torino, 2008;

BANDYOPADHYAY D., SEN J., *Internet of Things: Applications and Challenges in Technology and Standardization*, in *Wirel. Pers. Commun*., vol. 58, no. 1, pp. 49–69, 2011;

BARABASI A.L., *Link. La nuova scienza delle reti*, Einaudi, Milano, 2004;

BARBATO V., LAGO G., MANZARI V., *Come ovviare al vuoto sui prelievi coattivi creato dalla sentenza n. 238 del 1996*, in *Dir. pen .e proc*, n. 3, 1997;

BARBIERI A., *Le attività d'indagine della polizia giudiziaria su sistemi informatici e telematici*, in *Dir. Internet, 2008, 5*;

BARGIS M., *Note in tema di prova scientifica nel processo penale*, in *Riv. D. Proc*., 2011, pp. 47 e ss;

BARNI M., TONDI B., *The source identification game: an information-theoretic perspective*, in *Information Forensics and Security, IEEE Transactions* on 8.3 (2013), pp. 450-463;

BARTOLI L., *La catena di custodia del materiale informatico: soluzioni a confronto*, in *Anales de la facultad de derecho*, 33; 2016, pp. 145-162;

BARTOLI L., *Parità delle armi e discovery digitale: qualche indicazione da Strasburgo*, in *www.lalegislazionepenale.it*, 13.1.2022;

BASILE F., *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. uomo*, 2019, 10;

BATTIATO S., BRUNA A., PUGLISI G., *A Robust Block Based Image/Video Registration Approach for Mobile Imaging Devices*, in *IEEE Transactions on Multimedia*, 2010, 12,7, pp. 622-635;

BATTIATO S., GALVAN F., *Ricostruzioni di informazioni 3D a partire da immagini bidimensionali*, in *Sicurezza e Giustizia* n. IV /MMXIII - pp. 12-14 (2013);

BAUMAN Z., *Dentro la globalizzazione*, Laterza, Bari, 1998;

BELFATTO E., *La biometria applicata alla sicurezza e al contesto forense*, FDE Institute Press, Mantova, 2015;

BEN ARI D., FRISH Y., LAZOVSKI A., ELDAN U., GREENBAUM D., *Artificial Intelligence in the Practice of Law: An Analysis and Proof of Concept Experiment*, in *23 Richmond Journal of Law & Technology*, 2017, p. 21 e ss.;

BENTHAM J., *Panopticon ovvero la casa d'ispezione*, Marsilio, Venezia, 1983;

BERNASCONI A., *La ricognizione di persone nel processo penale. Struttura e procedimento probatorio*, Giappichelli, Torino, 2003;

BERNSTEIN D. E., *Junk Science in the United States and the Commonwealth*, in *Yale J. Int. L.*, 1996;

BERTILLON A., *Identification anthropometrique: instruction signaletiques*, Melun, Imprimerie Administrative, 1893;

BERTILLON A., *La Photographie Judiciaire*. Gauthier-Villars et fils, Paris, 1890;

BESTAGINI P., ALLAM A., MILANI S., TAGLIASACCHI M., TUBARO S., *Video codec identification*, in *IEEE International Conference on Acoustics, Speech, and Signal Processing* (ICASSP), (2012);

BESTERS M., BROM F.W.A., *"Greedy" Information Technology: The Digitalization of the European Migration Policy*, in *European Journal of Migration & Law*, 12, 4, 2010, p. 462;

BIRAL M., *L'identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, in *Rivista Italiana di Diritto e Procedura Penale*, fasc. 4, 2015, p. 1842;

BISI S., *Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica*, in *Ciberspazio e diritto*, 6 (4), pp. 3-35;

BISSI S., *Biometria e videosorveglianza*, in http://archivio.cnipa.gov.it/site/_files/2007120629641.pdf ;

BIZZARRO P.G., *Il futuro è nei dati: data sharing e data spaces nel mercato unico europeo*, disponibile su https://datavalley.it/2021/04/07/il-futuro-e-nei-dati-data-sharing-e-data-spaces-nel-mercato-unico europeo/?fbclid=IwAR3ofkdNg5hQzJeQyMjhYigAqfn0I6vHbH21-pxAFa7i8JgALELpFdRlEbw;

BODEN M.A., *L'intelligenza artificiale*, Il mulino, Bologna, 2019;

BOLLE R.M., CONNELL J.H., PANKANTI S., RATHA N.K., SENIOR A.W., *Guide to Biometrics*. Springer-Verlag, New-York, 2003;

BONETTI M., *Riservatezza e processo penale*, Giuffrè, Milano, 2003;

BÖSE M., *An Assessment of the Commission's Proposal on Electronic Evidence*, reperibile all'inidirizzo https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf;

BOVE T., GIUA P.E., FORTE A., ROSSI C., *Un metodo statistico per il riconoscimento del parlatore basato sull'analisi delle formanti*, in *Statistica*, anno LXII, n. 3, 2002;

BOZIO V., *L'ammissibilità nel processo penale di videoriprese effettuate dalla persona offesa*, in *Dir. pen. proc.*, 2015, p. 585 ss.;

BRAMANTI M., *Valutazioni probabilistiche sui riscontri del DNA a scopo di identificazione criminale*, in *La Matematica nella Società e nella Cultura - Rivista dell'Unione Matematica Italiana*, Serie I, Vol. II, n. 3, Dicembre 2009;

BRANDEIS L.D., WARREN S., *The Right of privacy*, in *4Harvard Law Review*, 1890, (tradotto da) S. Serra, in *Ius solitudinis*, (a cura di) V. Frosini, Giuffrè, Milano, 1993;

BRAVO A., *Argomenti di Grafologia peritale*, E.S.I., Napoli, 2001;

BRAVO A., *Metodologia della consulenza tecnica e della perizia grafica*, Giordano Editore, Mesagne, 2005;

BRAVO A., *Variazioni naturali e artificiose della grafia*, Giordano Editore, Mesagne, 2005;

BRECKENRIDGE K., *Biometric State. The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*, Cambridge University Press, 2014;

BRKAN M., *Do algoritms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond*, in *Electronic Journal*, gennaio 2017;

BROMBA M., *On the Reconstruction of Biometric Raw Data from Template Data*, (2006) *https://www.bromba.com/knowhow/temppriv.htm* (visualizzato in data 12.10.2021);

BRUSCO C., *Il vizio di motivazione nella valutazione della prova scientifica*, in *Dir. pen. proc*., 2004, 14, 1414;

BRUSCO C., *La valutazione della prova scientifica*, in *Dir. pen. proc*., 2008, Dossier: La prova scientifica nel processo penale;

BRUSCO C., *Scienza e processo penale: brevi appunti sulla valutazione della prova scientifica*, in *Riv. it. medicina legale (dal 2012 Riv. it. medicina legale e dir. sanitario*), fasc.1, 2012, p. 61;

BUDOWLE B. *et al*., *CODIS and PCR-Based Short Tandem Repeat Loci: Law Enforcement Tools*, in *Promega Corporation (ed) Genetic Identity Conference Proceedings of the Second European Symposium on Human Identification*, pp. 73-88, (Madison, WI);

BUOLAMWINI J., ORDÓÑEZ V., MORGENSTERN J., LEARNED-MILLER E., *Facial Recognition Technologies: A Primer*, in *Algorithmic Justice League*, 2020;

CABIALE A., *I limiti alla prova nella procedura penale europea*, Wolters Kluwer, Cedam, Padova, 2019;

CABIALE A., *L'Acquisizione delle intercettazioni con procedura di controllo giudiziale: ritorni al passato e nuove lacune*, in *Diritto di Internet, digital copyright and data protection*, suppl. fasc. 3/2020;

CAIANIELLO M., *Dal terzo pilastro ai nuovi strumenti: diritti fondamentali, "road map" e l'impatto delle nuove direttive*, in *I nuovi orizzonti della giustizia penale europea, Atti del convegno*. Milano, 24-26 ottobre 2014, Milano, 2015;

CAIANIELLO M., *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 29 (2021) 1-23;

CAIANIELLO M., *L'OEI dalla direttiva al decreto n. 108 del 2017*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017*, (a cura di) M. Daniele, R.E. Kostoris, Giappichelli, Torino, 2018;

CAIN S., SMRKOVSKY L., WILSON M., *Voiceprint Identification*, si veda http://expertpages.com/news/voiceprint_identification.html;

CAJANI F., *Il vaglio dibattimentale della digital evidence*, in *Arch. pen.*, 2013 fascicolo 3 anno LXV, pp. 837–852;

CALAMANDREI P., *Il giudice e lo storico*, in *Riv. dir. proc*., 1939;

CALAVITA O., *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, in *www.lalegislazionepenale.it*, 30.3.2021;

CALOGERO G., *La logica del giudice e il suo controllo in Cassazione*, Cedam, Padova, 1937;

CAMALDO L., *La direttiva sull'ordine europeo di indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione*, in *Dir. pen. cont*., 27.5.2014.

CAMON A., *La disciplina delle indagini genetiche*, in *Cass. pen*., fasc. 4, 2014, p. 1426B;

CAMON A., *La prova genetica tra prassi investigative e regole processuali*, in *Proc. pen. giust*., 2015, n. 6, pp. 165 e ss.;

CAMON A., *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen*., fasc.4, 1999, p. 1188;

CAMON A., *Le Sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi*, in *Riv. it. dir. proc. pen*., 2006, p. 1550;

CANZIO C., *Prova scientifica, ricerca della "verità" e decisione giudiziaria nel processo penale*, in AA.VV., *Scienza e casualità*, (a cura di) C. De Maglie, S. Seminara, Cedam, Padova, 2006;

AA.VV., *Prova scientifica e processo penale*, (a cura di) G. Canzio, L. Luparia, Wolters Kluwer - Cedam, Milano, 2018;

CANZIO G., *Intelligenza artificiale e processo penale*, in *Cass. pen.*, fasc.3, 2021, p. 797;

CANZIO G., *Intelligenza artificiale, algoritmi e giustizia penale*, in *www.sistemapenale.it*, 8.1.2021;

CANZIO G., *L'"oltre il ragionevole dubbio" come regola probatoria e di giudizio nel processo penale*, in *Riv. it. dir. proc. pen*., 2004, p. 305;

CANZIO G., *La causalità fra diritto e processo penale*, in *Cass. pen*., 2007, p.1324;

CANZIO G., *Prova scientifica, ragionamento probatorio e libero convincimento del giudice nel processo penale*, in *Dir. pen. proc*., 2003, p. 1200;

CAPRIOLI F., *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen*., 2009, p. 3520;

CAPRIOLI F., *Scientific evidence e logiche del probabile nel processo per il "delitto di Cogne"*, in *Cass. pen*., 2009, p. 1866;

CAPRIOLI F., *Verità e giustificazione nel processo penale*, in *Revista Brasileira de Direito Processual Penal*, vol. 3, n. 1, 2017;

CARETTI P., DE SIERVO V., *Istituzioni di diritto pubblico*, Giappichelli, Torino, 2006;

CARLI GARDINO A., *Il diritto di difesa nell'istruttoria penale: saggio sull'art. 24 comma 2 Cost.*, Giuffrè, Milano, 1983;

CARLIZZI G., TUZET, *La prova scientifica nel processo penale*, Giappicchelli, Torino, 2018;

CARLIZZI G., *Giudice 2.0 e uso del sapere specialistico nel processo penale*, in *Processo penale e giustizia* n. 4/2017, pp. 732-754;

CARLIZZI G., *La valutazione della prova scientifica*, Giuffrè, Milano, 2019;

CARNELUTTI F., *La prova civile*, Roma, 1915;

CARNELUTTI F., *Lezioni sul processo penale*, vol. I, Roma, 1946;

CARNELUTTI F., *Principi del processo penale*, Giuffrè, Milano, 1960;

CARNELUTTI F., *Prova del sangue*, in *Riv. dir. proc*., 1961, pp. 129 e ss;

CAROFIGLIO G., *L'arte del dubbio*, Palermo, 2007;

CARPONI SCHITTAR D. H. L., *Modi dell'esame e del controesame*, vol. I, Giuffrè, Milano, 1992;

CARRETTA P., CILLI A., IACOVIELLO A., GRILLO A., TROCCHI F., *L'acquisizione del documento informatico. Indagini penali e amministrative*, Laurus Robuffo, Roma, 2012;

CARRIER B.D., *Defining digital forensic examination and analysis tool using abstraction layers*, in *International Journal of Digital Evidence*, 1, 2003, 4, pp. 1-12;

CARVALHO D.V., PEREIRA E.M., CARDOSO J.S., *Machine Learning Interpretability: A Survey on Methods and Metrics*, in *Electronics*, 2019, 8, 832;

CASASOLE, F., *Le indagini tecnico-scientifiche: un connubio tra scienza e diritto in perdurante attesa di disciplina*, in *Dir. Pen. e Processo*, 2008, 11, 1443;

CASCETTA F., DE LUCCIA M., *Sistemi d'identificazione personale*, in *Il mondo Digitale*, 2004, reperibile all'indirizzo http://archivio-mondodigitale.aicanet.net/Rivista/04_numero_due/Cascetta_p.44-55.pdf ;

CASEY E., *Digital Evidence and Computer Crime. Forensic science, computer and the Internet*, Second Edition, Elsevier Academic Press, Amsterdam, 2004;

CASONATO C., *Intelligenza artificiale e giustizia: potenzialità e rischi*, in *DPCE Online*, v. 44, n. 3, 2020;

CASSANO G., CIMINO I.P., *Diritto dell'internet e delle nuove tecnologie telematiche*, Cedam, Padova, 2009;

CASTELLI C., PIANA D., *Giustizia predittiva. La qualità della giustizia in due tempi*, in *Quest. Giust.* (web), 3 luglio 2019;

CATALANO E., *L'accertamento dei fatti processuali*, in *Ind. pen*., 2002;

CATANESI R., MARTINO V., *Verso una psichiatria forense basata su evidenza*, in *Riv. it. med. leg*., 2006, p. 1011;

CATH C., WACHTER S., MITTELSTADT B., TADDEO M., FLORIDI L., *Artificial Intelligence and the 'Good Society': the US, EU, and UK approach*, in *Science and Eng. Ethics*, 2018;

CECCHI M., *La "motivazione rafforzata" del provvedimento ovvero la "forza persuasiva superiore"*, in *DPP*, 2019, 1123 ss;

CENTONZE F., *Scienza "spazzatura" e scienza "corrotta" nelle attestazioni e valutazioni dei consulenti tecnici nel processo penale*, in *Riv. it. dir. proc. pen.*, 2001, pp. 1232 ss;

CESARI C., *L'impatto delle nuove tecnologie sulla giustizia penale- un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal, Porto Alegre,* vol. 5, n. 3, pp. 1167-1188;

CESARI C., *L'irripetibilità sopravvenuta degli atti di indagine,* Giuffrè, Milano, 1999;

CHAN G.K.Y., *Towards a calibrated trust-based approach to the use of facial recognition technology*, in *International Journal of Law and Information Technology*, 2021, 00, pp. 1-27;

CHANG Y., ZHANG W., CHEN T., *Biometric-based cryptographic key generation,* in *Proceedings of IEEE International Conference on Multimedia and Expo (ICME'04)*, Taipei, vol. 3, 2004, pp. 2203–2206

CHAPMAN R. B., *Admissibility of Voiceprints Not Limited to "Corroborative Purposes", United States v. Franks*, 511 F.2d 25 (6th Cir. 1975), in *Akron Law review*, si veda: https://www.uakron.edu/dotAsset/d1e99bd8-b0df-40b3-9637-1a9084acb737.pdf;

CHELO A., *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, Cedam, Milano, 2014;

CHIAVARIO M., *Considerazioni sul diritto alla prova*, in *Cass. pen*., 1996, p. 2009;

CHIAVARIO M., *Diritto processuale penale,* 8° ed., Utet giuridica, Milano, 2019;

CHIAVARIO M., *Diritto processuale penale,* 9° ed., Utet giuridica, Milano, 2022;

CHIAVARIO M., *Diritto processuale penale. Profilo istituzionale,* II ed., UTET, Torino, 2006;

CHIAVARIO M., *La riforma del processo penale,* 2° ed., Giappichelli, Torino, 1990;

CHIAVARIO M., *Libertà personale (dir. proc. pen.)*, in *Enc. giur. Treccani*, Roma, 1993;

CHIAVARIO M., *Processo e garanzie della persona*, vol. II, Giuffrè, Milano, 1984;

CHIAVARIO M., *sub art. 6 Cedu*, in S. Bartole, B. Conforti, G. Raimondi, *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, Cedam, Padova, 2001;

CHIAVARIO M., *voce "Giusto processo" (processo penale)*, in *Enciclopedia giuridica Treccani*, Roma, 2001, 1;

CISTERNA A., *Perquisizioni in caso di fondato motivo*, in *Guida dir*., 2008;

CLARKE R., *Biometric's Inadequacies and Threats, and the Need for the Regulation*, 15 aprile 2002, disponibile su http://www.rogerclarcke.com/DV/BiomThreats.html;

COATS W. S., BAGDASARIAN A., HELOU T. J., LAM T., *The Practitioner's Guide to Biometrics*, American Bar Association, Chicago, 2007;

COLAIOCCO A., *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria,* in *Arch. Pen*., Fasc. n. 1 – Gennaio-Aprile 2019 (online);

COLAROCCO V., GROTTO T., VACIAGO G., *La prova digitale. La casistica civile e penale e gli strumenti di acquisizione in ambito* cloud, Giuffrè, Milano, 2020;

COLE S. A., *Is Fingerprint Identification Valid? Rhetorics of Reliability in Fingerprint Proponents'Discourse*, in *Law & Policy*, Vol. 28, No. 1, January 2006, p. 116;

COLOGGI F., *Identità personale: filosofia, scienza e criminologia*, in *Profiling. I profili dell'abuso. Giornale scientifico a cura dell'O.N.A.P.*, Anno 1, N. 4, dicembre 2010, in http://www.onap-profiling.org/?p=853;

COLOMBO E., *Una novità dall'Unione Europea per la lotta ai Cybercrimes: una Electronic Evidence Guide*, in *Cass. pen.*, 2014, pp. 374 e ss.;

COMOGLIO L. P., *Prove ed accertamento dei fatti nel nuovo c.p.p.*, in *Riv. it. dir. proc. pen*., 1990, p. 119;

CONFORTI A., *Controesame di testi della controparte su circostanze non indicate e nuove interpretazioni del diritto alla prova contraria*, in *Cass. pen*., 1998, p. 2038;

CONSO G., *Considerazioni in tema di contraddittorio nel processo penale italiano*, in *Riv. it. dir. proc. pen*., 1966, p. 405;

CONSO G., GREVI V., NEPPI MODONA G., *Il nuovo codice di procedura penale. Dalle leggi delega ai decreti delegati*, vol. IV, Cedam, Padova, 1989;

CONSO G., *I fatti giuridici processuali penali*, Milano, 1955;

CONSO G., V. GREVI, G. NEPPI MODONA, *Il nuovo codice di procedura penale. Dalle leggi delega ai decreti delegati*, vol. I, Padova, 1989;

CONSOLO O., *voce Perito ed interprete (dir. proc. pen.)*, in *Enc giur. Treccani*, vol. XIII, Roma, 1990, p. 2;

CONTALDO A., *Biometrie e documenti di viaggio: problematiche giuridiche in campo*, in *Rivista Amministrativa della Repubblica Italiana*, 2006, 6, pp. 545 ss.;

CONTI C., *Il processo si apre alla scienza. Considerazioni sul procedimento probatorio e sul giudizio di revisione*, in *Riv. It. Dir. Proc. Pen*., 2010, pp. 1204 ss.;

CONTI C., *Il volto attuale dell'inutilizzabilità: derive sostanzialistiche e bussola della legalità*, in *Dir. pen. proc*., 2010, pp. 790 e ss.;

CONTI C., *La riservatezza delle intercettazioni nella "delega Orlando"*, in *www.dirittopenalecontemporaneo.it*, 2017 (3), pp. 78 ss.;

CONTI C., *Le due anime del contraddittorio nel nuovo art. 111 Cost.*, in *Dir. pen. proc*., 2000;

CONTI C., *Le videoriprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi "riservati"*, in *Dir. pen. proc*., 2006, pp. 1347 ss.;

CONTI C., *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Diritto penale e processo*, 9/2018, pp. 1210 e ss.;

CONTI C., *Scienza controversa e processo penale: la Cassazione e il "discorso sul metodo"*, in *Dir. pen. e processo*, 2019, 6, 848;

CONTI C., *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, Giuffrè, Milano, 2011;

CONTI C., TONINI P., *Il diritto delle prove penali*, Giuffrè, Milano, 2014;

CONTI S., *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, pp. 153-164;

CONTI S., PERUGINELLI G., *L'impatto del regolamento europeo in materia di protezione dei dati personali sull'attività giurisdizionale*, in *Ciberspazio e Diritto*, 1-2, 2018, pp. 123 ss.;

CORASANITI M., *La banca dati del DNA: primi aspetti problematici dell'attuazione del Trattato di Prüm*, in *Dir. informatica*, fasc.3, 2009, p. 437;

CORBETTA S., *Commento all'art. 508 c.p.p.*, in AA.VV., *Codice di procedura penale commentato*, (a cura di) GIARDA A., G. SPANGHER G., Ipsoa, Milano, 2007, pp. 4478 e ss.;

CORDERO F., *Codice di Procedura penale commentato*, Giappichelli, Torino, 1990;

CORDERO F., *Ideologie del processo penale*, Giuffrè, Milano, 1966;

CORDERO F., *Procedura penale*, Giuffrè, Milano, 2003;

CORDERO F., *Procedura penale*, Giuffrè, Milano, 2012;

CORDERO F., *Tre studi sulle prove penali*, Giuffrè, Milano, 1963;

COSTABILE G., *Scena criminis, documento informatico e formazione della prova penale, Il diritto dell'Informazione e dell'Informatica*, in *Il diritto dell'informazione e dell'informatica*, 2005;

CREEMERS R., *China's Social Credit System: An Evolving Practice of Control*, in *SSRN*, 9.5.2018, pp. 1-32;

CREMONESI L., *Indagini e garanzie nel sistema americano*, Laurus Robuffo, Roma, 2010;

CUOMO L., RAZZANTE R., *La nuova disciplina dei reati informatici*, Giappichelli, Torino, 2009;

CUOMO L., *Profili giuridici del trattamento biometrico dei dati*, in *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)*, fasc.1, 2014, p. 43;

CURRAO E., *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *DPU*, 19.5.2021;

CURTI S., FALCINELLI D., *Tra diritto e scienza: i saperi e la prova nel processo penale*, Cedam, Padova, 2014;

CURTOTTI NAPPI D., SARAVO L., *L'errore tecnico-scientifico sulla scena del crimine. L'errore inevitabile e le colpe dello scienziato, del giurista, del legislatore*, in *Arch. pen.*, 2011, n. 3;

CZERNIAWSKI J., BOYACK C., *Reviewing the Privacy Implications of Law Enforcement Access to and Use of Digital Data*, in *5 UTAH J. CRIM. L.* 73 (2021);

D'AMBROSIO L., VIGNA P. L., *La pratica di polizia giudiziaria*, Cedam, Padova, 1998;

D'ARIENZO A**.,** *Raccolta di appunti di criminalistica*, in *Sez. Identità Personale – Dattiloscopia*, disponibile su www.officeitalia.it/scicosi/datt.html;

D'AURIA L., *Accertamento oltre il ragionevole dubbio, rispetto del contraddittorio e criteri di verifica dell'attendibilità delle ipotesi scientifico tecniche come principi fondanti il "giusto processo". Risvolti sulla prova penale scientifica e gli accertamenti tecnici*, in *Foro ambr*., 2003;

D'AURIA L., *Blood pattern Analisys e ragionamento del giudice*, in *Giust. pen*., 2006, c. 220;

D'AURIA L., *Prova penale scientifica e "giusto processo"*, in *Giust. pen*., 2004, c. 20.

DALFINO D., *Stupidità (non solo) artificiale, predittività e processo*, in *Quest. Giust*. (web), 3 luglio 2019;

DAMASKA, M., *Il diritto delle prove alla deriva*, Il Mulino, Bologna, 2003;

DANIELE M., *Habeas Corpus. Manipolazioni di una garanzia*, Giappichelli, Torino, 2017;

DANIELE M., *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen*., 2012;

DANIELE M., *Indagini informatiche lesive della riservatezze. Verso un'inutilizzabilità convenzionale?*, in *Cass. pen*., 2013, pp. 367 ss..;

DANIELE M., *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Rev. Bras. de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, pp. 1277-1296, 2019;

DANIELE M., *L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul d. lgs. n. 108 del 2017*, in *Dir. Pen. Cont*., 7-8/2017, pp. 208 e ss.;

DANIELE M., *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale*, in *Dir. pen. cont. – Riv. trim*., 2015, n. 4, pp. 86 s.;

DANIELE M., *La prova digitale nel processo penale*, in *Riv. dir. proc*. 2/2011, pp. 284 e ss.;

DE CATALDO NEUBERGER L., *Esame e controesame nel processo penale. Diritto e psicologia*, 2° ed., Cedam, Padova, 2008;

DE CATALDO NEUBERGER L., *Psicologia della testimonianza e prova testimoniale*, Giuffrè, Milano, 1988;

DE GREGORIO G., *The Digital Services Act: A Paradigmatic Example of European Digital Constitutionalism*, in *Diritti Comparati*, 17.5.2021, pp. 1-6;

DE HERT P., *Biometrics: legal issues and implications, in Background paper for the Institute of Prospective Technological Studies*, in *DG JRC – Sevilla, European Commission*, 2005;

DE LEO F., *Le indagini tecniche di polizia: un invito al legislatore*, in *Cass. Pen*., 1996 pp. 697 ss.;

DEGANELLO M., *I criteri di valutazione della prova penale. Scenari di diritto giurisprudenziale*, Giappichelli, Torino, 2005;

DELAC K., GRGIC M., *A survey of biometric recognition methods*, in *46th International Symposium Electronics in Marine, ELMAR-2004*, 2004, Zadar, Croatia;

DELLA TORRE J., *Novità dal regno unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del garante privacy d'oltremanica)*, in *www.sistemapenale.it*, 28.3.2020;

DENTI V., *Scientificità della prova e libera valutazione del giudice*, in *Riv. dir. proc*., 1972;

DEVARAM R. R., ORTIS A., BATTIATO S., BRUNA A. R., TOMASELLI V., *Real-Time Thermal Face Identication System for Low Memory Vision Applications Using CNN*, in *Pattern Recognition. ICPR International Workshops and Challenges*, Springer Professional, 2021;

DEWEY M., *Classificazione decimale Dewey*, (a cura di) CROCETTI L., DANESI D., Vol. II, AIB, Roma, 1993;

DI CHIARA G., *Le linee prospettiche del difendersi ricercando: luci e ombre delle "nuove" investigazioni difensive*, in *Leg. pen*., 2002, pp. 20 ss.;

DI NICOLA V., *La libertà personale dell'imputato tra regole smesse, disciplina attuale e sistema futuro*, Boccia, Salerno, 1989;

DI PAOLO G., *La circolazione dei dati personali nello spazio giudiziario europeo dopo Prüm*, in *Cass. pen.*, 2010, pp. 1969 e ss.;

DI PAOLO G., *Tecnologie del controllo e prova penale. L'esperienza statunitense e spunti per la comparazione*, Cedam, Padova, 2008;

DI PAOLO G., *voce Prova informatica (diritto processuale penale)*, in *Enc. Dir*., Annali, VI, Giuffrè, Milano, 2013;

DIXON P., *A Failure to "Do No Harm". India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in *Health Technol.* 7, 2017, pp. 539–567;

DOBOSZ M., CARNEVALI E., LANCIA M., *Genetica forense e diritto: prospettive scientifiche, tecnologiche e normative*, Giuffrè, Milano, 2011;

DODGE D., *Novel Warrant IDS Suspect Only by DNA Databank Evidence Used to Charge «John Doe» Rape*, in *Milwakee J.E. Sentinel*, 1999;

DOMENICI R., *Prova del DNA*, in *Dig. disc. pen*., vol. X, Torino, 1995;

DOMINIONI O., *In tema di nuova prova scientifica*, in *Dir. pen. proc*., 2001;

DOMINIONI O., *L'esperienza italiana di impiego della prova scientifica nel processo penale*, in *Dir. Pen. e Processo*, 2015, 5, 601;

DOMINIONI O., *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2005;

DOMINIONI O., *sub art. 27 comma 2 Cost*., in AA. VV., *Commentario della Costituzione*, (a cura di) BRANCA G., Bologna-Roma, 1991, pp. 212 ss.;

DONATI F., *Intelligenza artificiale e giustizia*, in *Rivista AIC*, 1/2020, 2.3.2020, pp. 415 e ss.;

DONDI A., *Paradigmi processuali ed "expert witness testimony" nel diritto statunitense*, in *Riv. trim. dir. proc. civ.*, 1996, pp. 261 ss.;

DONDI E., *Problemi di utilizzazione delle "conoscenze esperte" come expert witness testimony nell'ordinamento statunitense*, in *Riv. trim. dir. proc. civ*., 2001, pp. 1191 ss.;

DUGELAY J.L., JUNQUA J.C., KOTROPOULOS C., KUHN R., PERRONNIN F., PITA I., *Recent advances in biometric person authentication*, vedi http://www.eurecom.fr/fr/publication/830/download/mm-dugeje-020513.pdf;

DUTTA A., *Predicting Performance of a Face Recognition System Based on Image Quality*, PhD thesis, University of Twente, Netherlands, 2015;

EBERS M., HOCH V.R.S., ROSENKRANZ F., RUSCHEMEIER H., STEINRÖTTER B., *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society*, in *(RAILS). J.*, 2021; 4(4), pp. 589-603;

EL-KHOBBY R., ABD-ELNABY H.A., et al., *Gait identification by convolutional neural networks and optical flow*, in *Multimed Tools Appl* 78**,** 25873–25888 (2019);

EVAN S., *Biometrics bring new benefits and challenges*, in *Electronic Design*, Vol.53 Issue 14, 6/30/2005;

FAGGIOLI G., GHIRARDINI A., *Computer Forensics*, Apogeo, Milano, 2009;

FAIGMAN D., *Legal alchemy. The use and the misuse of the science in the law*, W. H. Freeman & Co, New York, 2001;

FAIGMAN D.L., E. PORTER, M.J. SACKS, *Cheek your Cristal Ball at the Courthouse Door, Please: Exploring the Past, Understanding the Present, and Worrying about the Future of Scientific Evidence*, in 15 *Cardozo L. Rev.* 1803 (1994);

FALATO F., *L'inferenza generata dai sistemi esperti e dalle reti neurali nella logica giudiziale*, in *Arch. pen*., 2020, 2;

FALETTI E., *Face detection*: *per la prima volta il riconoscimento al vaglio dei tribunali*, in *Il Quotidiano giuridico*, 29.10.2019;

FANCHIOTTI V., *Lineamenti del processo penale statunitense*, Giappichelli, Torino, 1987;

FANUELE C., *Dati Genetici e procedimento penale*, Cedam, Padova, 2009;

FANUELE C., *L'indagine genetica nell'esperienza italiana ed in quella inglese*, in *Riv. it. dir. proc. pen*., 2006, pp. 732 ss.;
FASOLIN S., *La copia di dati informatici nel quadro delle categorie processuali*, in *Dir. pen. proc*., 2012;

FATTORINI P., CORRADI F., RICCI U., PREVIDERÈ C., *La prova del Dna per la ricerca della verità. Aspetti giuridici, biologici e probabilistici*, Giuffrè, Milano, 2006;

FELICIONI P., *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Ipsoa, Milano, 2007;

FELICIONI P., *Art. 188*, in AA.VV., *Codice di procedura penale commentato*, (a cura di) A. Giarda, G. Spangher, I, Wolters Kluwer, Milano, 2017, pp. 1872 ss;

FELICIONI P., *L'Italia aderisce al Trattato di Prüm: disciplinata l'acquisizione e l'utilizzazione probatoria dei profili genetici*, in *Dir. pen. proc., 2009, Dossier: Banca dati nazionale del DNA e prelievo di materiale biologico*;

FELICIONI P., *La prova del Dna nel procedimento penale. Profili sistematici, dinamiche probatorie, suggestioni mediatiche*, Giuffrè, Milano, 2018;

FELICIONI P., *Le ispezioni e le perquisizioni*, Giuffrè, Milano, 2004;

FERRAJOLI L., *Diritto e Ragione – Teoria del garantismo penale*, Laterza, Bari, 1998;

FERRARESI M., *L'effetto CSI può fregare DSK*, in *Il Foglio*, 24 maggio 2011;

FERRUA P., *Il "giusto processo"*, Zanichelli, Bologna, 2010;

FERRUA P., *La prova nel processo penale, I, Struttura e procedimento*, Giappichelli, Torino, 2017;

FERRUA P., *Studi sul processo penale*, vol. II, *Anamorfosi del processo accusatorio*, Giappichelli, Torino, 1992;

FERRUA P., *voce Difesa (diritto di)*, in *Dig. disc. pen*., vol. III, 1989, p. 466;

FERRUA, P., *La prova nel processo penale*, Giappichelli, Torino, 2017;

FIDELBO G., *Le Sezioni unite riconoscono rilevanza ai disturbi della personalità*, in *Cass. pen*., 2005, p. 1850;

FILIPPI L., *Commento all'art. 266 bis c.p.p*., in AA.VV., *Codice di procedura penale commentato*, A. Giarda, G. Spangher, Ipsoa, Milano, 2007, p. 1921;

FILIPPI L., *L'intercettazione di comunicazioni*, Giuffrè, Milano, 1997;

FIORI A., *La prova in medicina legale*, in *Riv. it. med. leg*., 2004;

FIORI A., MARCHETTI D., *I garanti del sapere scientifico in sede giudiziaria*, in *Riv. it. Med. Leg*., 33, 489;

FIORI A., *Mito, realtà e fallacie del Dna (nella pratica forense)*, in *Rivista Italiana di Medicina legale e diritto sanitario*, fasc. 6, 2011, p. 1329;

FISHER G., *The Jury's Rise as Lie Detector*, in 107 *YALE L.J.* 575, 1997;

FLOR R., *La Corte di giustizia considera la Direttiva europea 2006/24 sulla cd. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. proc*., 2009, 403;

FLORA M. G. P., *Biometria e clonazione delle impronte digitali*, in *Dir. Internet*, 2006, 6, pp.1 ss.;

FLORIAN E., *Delle prove penali*, Cisalpino, Milano, 1961;

FLORIDI L., *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Raffaello Cortina Editore, Milano, 2022;

FLORIDI L., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano, 2014;

FLORIDI L., *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, *Philos. Technol.* 34, 2021, pp. 215–222;

FOCARDI F., *La consulenza tecnica extraperitale delle parti private*, Cedam, Padova, 2003;

FONSI A., *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time*, in *Penale Diritto e Procedura*, 13.5.2021;

FORMICI G., *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, in *Saggi – DPCE online*, 2019/2;

FOSTER W. L., *Expert testimony. Prevalent complaints and proposed remedies*, in *Harvard L. R.*, 1897, v. 11, p. 169;

FOUCAULT M., *Surveiller et punir. Naissance de la prison*, Editions Gallimard, Paris, 1975;

FRANZEN J., *Purity*, Einaudi, Torino, 2016;

FRECKLETON J., *Problems posed by Dna evidence: of blood, babies and bathwater*, 17 (1), in *Alternative Law Journal*, 10 (1992).

FREEMAN L., *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, in *Fordham International Law Journal*, Vol. 41, Issue 2, 283;

FRONZA E., CARUSO C., *Ti faresti giudicare da un algoritmo?, Intervista A. Garapon*, in *Quest. giust*. (web), 2018, 4, p. 196;

FUMAGALLI F., *Le tecnologie biometriche e il loro utilizzo*, in *IBM Technical Solutions*;

FURGIUELE A., *La prova per il giudizio nel processo penale*, Giappichelli, Torino, 2007;

GABRIELLI C., *"Accertamenti medici" dai confini troppo incerti*, in *Guida dir*., 2009, n. 30, p. 73;

GABRIELLI C., *Il prelievo coattivo di campioni biologici nel sistema penale*, Giappichelli, Torino, 2012;

GABRIELLI C., *La decisione del "prelievo" torna al giudice*, in *Guida dir*., 2009, n. 30, pp. 68 ss.;

GAITO A., *La prova penale*, Utet, Torino, 2008;

GALANTINI N., *L'inutilizzabilità della prova nel processo penale*, Cedam, Padova, 1992;

GALANTINI N., *voce Inutilizzabilità (dir. proc. pen.)*, in *Enc. dir*., vol. I agg., Milano, 1998, p. 648;

GALBALLY J., ROSS A., GOMEZ-BARRERO M., FIERREZ J., ORTEGA-GARCIA J., *Iris Image Reconstruction from Binary Templates: An Efficient Probabilistic Approach Based on Genetic Algorithms*, in *Computer Vision and Image Understanding*, Vol. 117, Issue 10, pp. 1512 - 1525, October 2013;

GALBOTTI S., *La libertà personale*, Giuffrè, Milano, 1953;

GALGANI B., *Habeas data e garanzie fondamentali*, in *Arch. pen. web*., 2019, 1;

GALLUCCIO MEZIO G., *Il prelievo di materiale biologico dalla persona sottoposta a restrizione della libertà personale in una recente pronuncia della Corte Suprema degli Stati Uniti*, in *Cass. pen.*, fasc. 5, 2014, p. 1874B;

GALTON F., *Biometry*, in *Biometrika*, Volume 1, Issue 1, October 1901, pp. 7–10;

GARAPON A., LASSÈGUE J., *La giustizia digitale. Determinismo tecnologico e libertà*, Il Mulino, Bologna, 2021;

GARBOLINO P., *Nuovi strumenti logici e informatici per il ragionamento giudiziario: le reti bayesiane*, in *Cass. pen*., 2007, p. 326;

GARBOLINO P., *Probabilità e logica della prova*, Giuffrè, Milano, 2014;

GARGANI A., *I rischi e le possibilità dell'applicazione dell'analisi del Dna nel settore giudiziario,* in *Riv. it. dir. proc. pen.,* 1993, p. 1310;

GARRET L., *Judging Innocence*, in *Columbia Law Review*, 2008, vol. 108, pp. 55 e ss;

GARVIE C., BEDOYA A., FRANKLE J., *The perpetual line-up: Unregulated police face recognition in America*, in *Georgetown Law, Center on Privacy & Technology*, reperibile all'indirizzo https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf;

GATES K. A., *Our Biometric Future. Facial recognition technology and the culture of surveillance*, New York University Press, 2011;

GENNARI G., *Bioinformazione e indagini penali: la l. 85 del 30 giugno 2009*, in *Resp. Civ.*, fasc. 12, 2009, p. 2630B;

GERACI R.M., *La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento E-evidence*, in *Cass. pen*., 2019, pp. 1340 e ss.

GERRA G., *Alcune tecniche di identificazione biometrica di pratica attuabilità*, in *Rivista giuridica sarda*, 2001;

GIALUZ M., DELLA TORRE J., *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir.pen.cont*., 2018, fasc. 5, pp. 277 e ss.;

GIALUZ M., *L'emergenza nell'emergenza: il decreto-legge n. 28 del 2020, tra ennesima proroga delle intercettazioni, norme manifesto e "terzo tempo" parlamentare*, in *www.sistemapenale.it*, 1 maggio 2020;

GIALUZ M., Premessa, in *Diritto di Internet, digital copyright and data protection*, suppl. fasc. 3/2020;

GIALUZ M., *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra stati uniti ed europa*, in *DPC online*, 29 maggio 2019;

GIALUZ M., *Radiologia e accertamenti medici coattivi: il difficile equilibrio tra libertà della persona ed esigenze di prova*, in *Riv. it. dir. proc. pen*., 2/2012, pp. 558-579;

GIANNELLI P. C., *The abuse of scientific evidence of criminal cases: the need for independent laboratories*, in *Virginia J. Social Policy & Law*, 1997, n. 4, pp. 439 ss.;

GIANNINI A.M., TIZZANI E., D'AMORE A., *L'identikit: come si aiuta un testimone a ricordare*, in *RIC- 4/2012*;

GIOSTRA G., *Analisi e prospettive di un modello incompiuto,* in *Quest. Giust*., 2001, p. 1130;

GIOSTRA G., *Gli importanti meriti e i molti limiti della nuova disciplina*, *Giur.it*., 2010, pp. 1219 e ss.;

GIOSTRA G., *voce Contraddittorio (principio del)*, in *Enc. giur*., Treccani, vol. VIII, Roma, 1988;

GIROTTO S., *Biometria e nanomedicina: le nuove frontiere della riconcettualizzazione tecnologica del corpo umano*, in *Nuova Giur. Civ*., 2009, 9, 20452;

GIROTTO S., *Trattamento di dati biometrici e dignità della persona*, in *La nuova giurisprudenza civile commentata*, 2012, 3, pp. 242 ss.;

GIULIANI A., *Il concetto di prova. Contributo alla logica giuridica*, Giuffrè, Milano, 1961;

GIULIANI A., *voce Prova (filosofia)*, in *Enc. dir*., vol. XXXVII, Milano, 1988, pp. 518;

GIULIANO A., *Dal pensiero di Lombroso all'impronta digitale. Passato e presente del metodo più efficiente, pratico e rapido d'identificazione personale*, Edizioni libreria Cortina, Torino, 2012;

GIUNCHEDI F., *Gli accertamenti tecnici irripetibili*, Giappichelli, Torino, 2009;

GIUNCHEDI F., *Le malpractices nella digital forensics. Quali conseguenze sull'inutilizzabilità del dato informatico?*, in *Arch. Pen*., 2013, 3, pp. 861 e ss.;

GIUNTA F., *Questioni scientifiche e prova scientifica tra categoria sostanziale e regole di giudizio*, in *Criminalia*, 2014;

GIUSTOZZI C., *Giuristi e informatici divisi da una lingua comune: autenticazione?*, reperibile all'indirizzo http://www.interlex.it/forum10/relazioni/24giustozzi.htm.;

GRAND J. S., *The blooding of America: Privacy and the Dna Dragnet*, in *23 Cardozo L. Rev*., 2002, 2277;

GRANJA R., AMORIM A., *Ethical challenges of merging criminal identification and civil identification within the Prüm system*, in *Forensic Science International: Genetics*, Vol. 57, 2022;

GRECO L., MANTELERO A., *Industria 4.0, robotica e privacy-by-design*, in *Diritto dell'Informazione e dell'In-formatica (Il)*, fasc.6, 1.12.2018, 875;

GREENWOOD V., *Sulla scena del crimine. Le nuove frontiere delle scienze forensi*, in *National Geographic*, Vol. 38, N.1, Luglio 2016;

GREVI V., *Alla ricerca di un processo penale giusto*, Giuffrè, Milano, 2000;

GREVI V., *Libertà personale e Costituzione*, Giuffrè, Milano, 1976;

GREVI V., *Nemo tenetur se detegere*: *interrogatorio dell'imputato e diritto al silenzio nel penale italiano***,** Giuffrè, Milano, 1972;

GREVI V., *voce Libertà personale dell'imputato*, in *Enc. dir.*, vol. XXIV, Milano Giuffrè, 1974;

GRIFANTINI F. M., *Inutilizzabilità*, in *Digesto* Quarta ed., Parte Penale, vol. III, Torino, 1993;

GRIFANTINI F. M., *La nozione di indizio nel codice di procedura penale*, in *Rivista di Diritto Processuale*, 1/2013, p. 12;

GRIJPINK J., *Privacy Law: Biometrics and Privacy*, (2001) 17(3), in *Computer Law & Security Review 154*, pp. 156-157 e ss.;

GROTHER P., NGAN M., HANAOKA K., *Face Recognition Vendor Test (FRVT). Part 2: Identification*, in *NIST*, dicembre 2020;

GUALTIERI P., *Prova informatica e diritto di difesa*, in *Dir. pen. proc.*, 2008;

GUARRIELLO V., *L'intelligenza artificiale tra profili giuridici ed alcune delle più attuali applicazioni al servizio della società*, reperibile all'indirizzo https://arsg.it/?p=1781 (visualizzato in data 27.7.2021);

GULOTTA G., *Psicologia della testimonianza*, in AA.VV., *Trattato di psicologia giudiziaria nel sistema penale*, (a cura di) G. Gulotta, vol. I, Milano, 1987, pp. 499 e ss.;

GULOTTA G., TUOSTO E.M., *Il volto nell'investigazione e nel processo. Nuova fisiognomica forense*, Giuffrè, Milano, 2017;

GUO G., MU G., RICANEK K., *Cross-age face recognition on a very large database: the performance versus age intervals and improvement using soft biometric traits*, in *Proc. 20th Int. Conf. Pattern Recognit*., Aug.2010, pp. 3392-3395;

HAACK S*., Legalizzare l'epistemologia. Prova, probabilità e causa nel diritto*, Università Bocconi, Milano, 2015;

HANSEN P.B., *Classic Operating Systems: From Batch Processing to Distributed Systems*, Springer, New York, 2001;

HÉNIN S., *AI. Intelligenza artificiale tra incubo e sogno*, Milano, 2019;

HILDEBRANDT M., *The Proposal for an EU AI Act of 21 April 2021, Brief Commentary*, 2021, reperibile all'indirizzo https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legalrequirements/F2662611_en (visualizzato in data 29.9.2021);

HRICK P., HEYDARI F., *The Growing World of Face Recognition Legislation: A Guide to Enacted and Proposed Legislation*, reperibile all'indirizzo https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5d9f7965391b2358bdccda63/1570732405589/The+Growing+World+of+Face+Recognition+Legislation.pdf;

HUBER P. W., *Galileo's revenge. Junk science in the Courtroom*, Basic books, New York, 1993;

IACONO, W. G., & LYKKEN, D. T., *The validity of the lie detector: Two surveys of scientific opinion*, in *Journal of Applied Psychology*, 82(3), 1997, 426–433;

IANNUZZI A., FILOSA F., *Il trattamento dei dati genetici e biometrici*, in *Dirittifondamentali.it* – Fasc. 2/2019;

IENCA M., *Intelligenza². Per un'unione di intelligenza naturale e artificiale*, Rosenberg & Sellier, Torino, 2019;

INTERNATIONAL BIOMETRIC GROUP, *How is «Biometrics» defined?*, in http://www.biometricgroup.com/reports/public/reports/biometric_definiti-on.html;

INTINI A., CASTO A. R., SCALI D.A., *Investigazione di polizia giudiziaria, Manuale delle tecniche investigative*, Laurus Robuffo, Roma, 2006;

INTRONA F., RAGO C., REGAZZO A., *Il giudice e il coraggio del dubbio*, in *Riv. it. med. Leg*., 1997, p. 447 ss.;

IOVANE G., MAGRO G., *STUDI-La biometria e nuovi sistemi di identificazione*, in *Rassegna dell'Arma dei Carabinieri*, Luglio-Settembre 2004, supplemento al n. 4;

JAFRI R., ARABNIA H.R., *A survey of face recognition techniques*, in *Journal of Information Processing Systems* 5, 2009, pp. 41–68;

JAIN A. K., BOLLE R., PANKANTI S., *Biometrics. Personal identification in Networked Society*, Kluwer Academic Publishers, Norwell, 1999.

JAIN A. K., NANDAKUMAR K., ROSS A., *50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities*, 2016, in http://biometrics.cse.msu.edu/pubs/gen_biometrics.html;

JAIN A. K., PANKANTI S., PRABHAKAR S., HONG L., ROSS A., WAYMAN J. L., *Biometrics: A Grand Challenge, Proceedings of International Conference on Pattern Recognition*, Cambridge, UK, Aug.2004,http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/Jainetal_BiometricsGrandChallenge_ICPR04.pdf ;

JAIN A. K., PANKANTI S., *Biometrics Systems: Anatomy of Performance*, in *IEICE TRANS. FUNDAMENTALS*, Vol. E00-A, NO, 2001;

JAIN A. K., ROSS A., *Bridging the Gap: From Biometrics to Forensics*, in *Philosophical Transactions of the Royal Society*, 2015. Disponibile in: http://rstb.royalsocietypublishing.org/content/370/1674/20140254;

JAIN A. K., ROSS A.A., NANDAKUMAR K., *Introduction to biometrics: a textbook*, Springer, Berlino, 2011;

JAIN A. K., *Biometrics: Past, Present and Future*, in *18th IAPR/IEEE Int.l Summer school for advanced studies on biometrics: BIOMETRICS FOR AI / AI FOR BIOMETRICS*, May 30 - June 4 2021;

JAIN A. K., ROSS A., PRABHAKAR S., *An Introduction to Biometric recognition*, in *IEEE Transactions on Circuits and Systems for Video Technology* 14(1):4 – 20;

JAIN A.K., DEB D., ENGELSMA J. J., *Biometrics: Trust, but Verify*, in *https://arxiv.org/abs/2105.06625*, 14 May 2021;

JACQUET M., CHAMPOD C., *Automated face recognition in forensic science: Review and perspectives*, in *Forensic Science International*, Vol. 307, 2020, pp. 1-14;

JASANOFF S., *La scienza davanti ai giudici. La regolazione giuridica della scienza in America*, Giuffrè, Milano, 2001;

JASSERAND C. A., *Avoiding terminological confusion between the notions of 'biometrics' and 'biometric data': an investigation into the meanings of the terms from a European data protection and a scientific perspective*, in *International Data Privacy Law*, 2016, Vol. 6, No. 1;

JASSERAND C., *Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data*, in *European Data Protection Law Review* 2, no. 3 (2016), pp. 297–311;

JASSERAND C., *New Extensive Guidelines on the Use of Facial Recognition by the Council of Europe*, in *EAB's Newsletter*, 2021;

JEFFREYS A.J., WILSON V., THEIN S.L., *Individual-Specific 'Fingerprints' of Human DNA*, in *Nature*, Vol. 316, 1985;

KALB L., *Il documento nel sistema probatorio*, Giappichelli, Torino, 2000;

KAPLAN J., *Intelligenza artificiale. Guida al futuro prossimo*, Luiss, Roma, 2017;

KAUBA C., KIRCHGASSER S., MIRJALILI V., UHL A., ROSS A., *Inverse Biometrics: Generating Vascular Images from Binary Templates*, in *IEEE Transactions on Biometrics, Behavior, and Identity Science* (T-BIOM), 2021;

KAUR H., KHANNA, P. *Biometric template protection using cancelable biometrics and visual cryptography techniques*, in *Multimed Tools Appl* 75, 16333–16361 (2016);

KAUR P., KRISHAN K., SHARMA S. K., KANCHAN T., *Facial-recognition algorithms: a literature review*, in *Medicine, Science and the Law*, 2020, vol. 60(2), pp. 131-139;

KAYE D. H., *A Fourth Amendament Theory for Arrestee Dna and other Biometric Databases*, in *University of Pennsylvania Journal of Constitutional Law*, Vol. 15, No. 4, pp. 1095-1160, April 2013;

KAYE D. H., *Statistics for lawyers and law for statistics*, in *89 Mich. L. Rev*., 1991, p. 1520;

KEENAN B., *Automatic Facial Recognition and the Intensification of Police Surveillance*, in *Modern Law Review*, 2021, 84(4), pp. 886–897;

KERR O., *Digital Evidence and the New Criminal Procedure*, in 105 *Columbia Law Review*, 2005;

KHAIRWA A., ABHISHEK K., PRAKASH S., T. PRATAP, *A comprehensive study of various biometric identification techniques*, in *2012 Third International Conference on Computing, Communication and Networking Technologies* (ICCCNT'12), 2012, pp. 1–6;

KHAN A.Z., RIZVI A., *AI based facial recognition technology and criminal justice: issues and challenges*, in *Turkish Journal of Computer and Mathematics Education*, Vol.12 No.14 (2021), pp. 3384-3392;

KHELIF K. ET AL., *Towards a Breakthrough Speaker Identification Approach for Law Enforcement Agencies: SIIP*, in *2017 European Intelligence and Security Informatics Conference (EISIC)*, 2017, pp. 32-39;

KHUN T. S., *La struttura delle rivoluzioni scientifiche. Come mutano le idee della scienza*, Einaudi, Torino, 1999;

KIM B., KHANNA R., KOYEJO O.O., *Examples are not enough, learn to criticize! Criticism for interpretability*, in *Advances in Neural Information Processing Systems*, MIT Press: Cambridge, MA, USA, 2016, pp. 2280 e ss.;

KIND C., *Containing the canary in the AI coalmine – the EU's efforts to regulate biometrics*, in *Ada Lovelace Institute*, 2021, reperibile all'indirizzo https://www.adalovelaceinstitute.org/blog/canary-ai-coalmine-eu-regulate-biometrics/;

KINDT E.S., *Having yes, using no? About the new legal regime for biometric data*, in *Computer Law and Security Review*, 34, 2018, pp. 523-538;

KITCHIN R., *The real-time city? Big data and smart urbanism*, in *GeoJournal*, 79, pp. 1–14;

KITCHIN R., *Thinking critically about and researching algorithms*, (2017) 20(1), in *Information, Communication and Society*, pp. 1-14;

KLEINBERG K.F., PHARM B., VANEZIS P.M.D., BURTON A.M., *Failure of Anthropometry as a Facial Identification Technique Using High-Quality Photographs*, in *Journal of Forensic Sciences*, 2007, 52(4), pp. 779 – 783;

KOEHLER J. J., CHIA A., LINDSEY S., *The random match probability in Dna evidence: irrelevant and Prejudicial*, in *Jurimetrics Journal*, 1995, pp. 201-218;

KOMARINSKI P., *Automated fingerprint identification systems* (AFIS), Elsevier Academic, Amsterdam, 2005;

KOOPS B.J., NEWELL B.C., TIMAN T., SKORVANEK I., CHOKREVSKI T., GALIC M., *A typology of privacy*, in *University of Pennsylvania Journal of International Law*, 2017;

KORTYLEWSKI A., EGGER B., SCHNEIDER A., GERIG T., MOREL-FORSTER A., VETTER T., *Analyzing and Reducing the Damage of Dataset Bias to Face Recognition With Synthetic Data*, in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, 2019, pp. 1-8;

KOSTORIS R.E., *Alt ai prelievi di sangue coattivi*, in *Dir. pen. e proc*., 1996, pp. 1094 e ss.;

KOSTORIS R.E., *I consulenti tecnici nel processo penale*, Giuffrè, Milano, 1993;

KOSTORIS R.E., *La lotta al terrorismo e alla criminalità organizzata tra speciali misure processuali e tutela dei diritti fondamentali nella Risoluzione del XVIII Congresso internazionale di diritto penale*, in *Riv. dir. proc*. 2010;

KRAUSOVÁ A., *Intersections between Law and Artificial Intelligence*, in *International Journal of Computer* (IJC) (2017) Volume 27, No 1, pp. 55-68;

KROLL J.A., J. HUEY, S. BAROCAS, E. W. FELTEN, J. R. REIDENBERG, D. G. ROBINSON & HARLAN YU, *Accountable Algorithms*, in 165 *U. PA. L. REV*. 633 (2017);

KUMAR A., KAUR N., *Face Recognition*, in *International Journal of Advanced Trends in Computer Applications (IJATCA)*, Vol. 3, no. 2, February - 2016, pp. 10-15;

LA MUSCATELLA D., *Il trattamento della prova digitale nel sistema processuale penale italiano. Anamnesi e prognosi di una patologia classica, declinata in una (apparente) riforma*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, pp. 263-279;

LA REGINA K., *L'identificazione della voce nel processo penale*, reperibile all'indirizzo https://www.letture.org/l-identificazione-della-voce-nel-processo-penale-katia-la-regina;

LA REGINA K., *L'identificazione della voce nel processo penale*, Wolters Kluwer, Milano, 2018;

LA REGINA K., *Riconoscimento della voce - brevi note sul riconoscimento della voce nel processo penale*, in *Giur. It.*, 2018, 1, 212;

LAGO G., *Banche dati del Dna: raccomandazioni internazionali, studio comparato con la Legge 85/2009*, in *Giust. Pen*., 2010, pp. 141 ss.;

LARONGA A., *Il pedinamento satellitare: un atto atipico lesivo di diritti inviolabili?*, in *Quest. giust*., 2002, p. 1153;

LASAGNI G., *Tackling phone searches in Italy and the United States: Proposals for a technological rethinking of procedural rights and freedoms*, in *New Journal of European Criminal Law*, 2018, 383– 401;

LAVALLE C., *La polizia non può costringere a sbloccare un iPhone protetto da FaceID o TouchID*, in *La Stampa*;

LAVANYA B., INBARANI H. H., *A Survey of Biometric Techniques*, in *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 5, Issue 7, July 2015;

LAVARINI B., *Elementi di procedura penale. Lezioni per il corso di laurea magistrale in chimica clinica, forense e dello sport*, Ecig Universitas, Genova, 2010;

LAVORGNA A., SUFFIA G., *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2/2021, pp. 88 e ss.;

LEE, Y., FILLIBEN, J.J., MICHEALS, R.J., PHILLIPS, P.J., *Sensitivity analysis for biometric systems: A methodology based on orthogonal experiment designs*, in *Computer Vision and Image Understanding* 117(5), 532–550 (2013);

LEO W., *What are the Effects of the Daubert Decision on Fingerprint Identification?*, disponibile su http://www.fingerprintidentification.net/sitebuildercontent/sitebuilderfiles/researchpaperondaubert1.pdf;

LESLIE D., *Understanding bias in facial recognition technologies*, *The Alan Turing Institute*, 2020;

LI S. Z., JAIN A. K., *Handbook of Face Recognition*, Springer, New York, 2011;

LI S.Z., JAIN A.K., *Encyclopedia of Biometrics*. Springer, Boston, 2015;

LIANG F., DAS V., KOSTYUK N., HUSSAIN M.M., *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, in *Policy and Internet*, 4, 10, 2018, pp. 415 ss;

LIEBMAN J. S., RIFKIND S. H., FAGAN J., WEST V., *A broken system: errors in capital causes 1973-1995*, Columbia University, 2000, disponibile su: http://www2.law.columbia.edu/instructionalservices/liebman/liebman_final.pdf;

LINARELLO P., *La banca dati nazionale del Dna*, in *Il Penalista*, 14 marzo 2016, si veda http://ilpenalista.it/articoli/indagini-scientifiche/la-banca-dati-nazionale-del-dna;

LIPTON Z.C., *The mythos of model interpretability*, in *arXiv*, 2016;

LOMBARDO, L., *La scienza e il giudice nella ricostruzione giudiziale del fatto*, in *Riv. dir. proc*., 2007, 35.

LORUSSO S., *Il contributo degli esperti alla formazione del convincimento giudiziale*, in *Arch. pen*., 2011, pp. 809 ss.;

LORUSSO S., *L'esame della scena del crimine nella contesa processuale*, in *Dir. pen. proc*., 2011;

LOZZI G., *Lezioni di procedura penale*, Giappichelli, Torino, 2010;

LOZZI G., *Lezioni di procedura penale*, Giappichelli, Torino, 2013;

LUCARELLI A., PICOZZI M., *Tracce criminali. Storie di omicidi imperfetti*, Mondadori, Milano, 2006;

LUIS GARCIA, R.D., ALBEROLA-LOPEZ C., AGHZOUT O., RUIZ-ALZOLA J., Biometric identification systems, in *Signal Processing* 83(12), 2539–2557 (2003);

LUPARIA L., ZICCARDI G., *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007;

LUPARIA L., *Computer crimes e procedimento penale*, in AA.VV., *Trattato di procedura penale*, (diretto da) G. Spangher, *Modelli differenziati di accertamento*, (a cura di) G. Garuti, Utet giuridica, Torino, 2011;

LUPARIA L., *I profili processuali*, in *Dir. pen. proc*., 2008;

LUPARIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48*, in *Dir. pen. proc*., 2008;

LUPARIA L., *Note conclusive nell'orizzonte d'attuazione dell'Ordine europeo di indagine*, in AA.VV., *L'ordine europeo di indagine. Criticità e prospettive*, (a cura di) T. Bene, L. Luparia, L. Marafioti, Giappichelli, Torino, 2016, pp. 249 s.;

LUPARIA L., *Privacy, diritti della persona e processo penale*, in *Riv. dir. proc*., 2019, 1464 s.;

LUPARIA L., G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007;

LYON L., *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2002;

LYON V.D., *Massima sicurezza. Sorveglianza e «guerra al terrorismo»*, Cortina Raffaello, Milano, 2005;

MAGGINO F., CICERCHIA G., *Algoritmi, etica e diritto*, in *Diritto dell'Informazione e dell'Informatica* (Il), fasc.6, 1.12.2019, p. 1161;

MAI G., CAO K., PONG C. YUEN AND JAIN A.K., *On The Reconstruction Of Face Images From Deep Face Templates*, in the *IEEE Transactions on Pattern Analysis and Machine Intelligence*;

MAIO D., MALTONI D., CAPPELLI R., WAYMAN J. L., AND JAIN A. K., *FVC2002: Fingerprint verification competition*, in *Proc. Int. Conf. Pattern Recognition (ICPR)*, Quebec City, QC, Canada, Aug. 2002, pp. 744–747;

MAIOLI C., *Dar voce alle prove: elementi di informatica forense, in Crimine virtuale, minaccia reale*, Franco Angeli, Milano, 2004;

MANES V., *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *Discrimen*, 15.5.2020;

MANFREDI V., PESSA E., *Il riconoscimento dei volti: aspetti cognitivi, neuropsicologici e computazionali*, in *Sistemi Intelligenti*, fasc. 3, dicembre 2011;

MARAFIOTI L., LUPARIA L. (a cura di), *Banca dati del Dna e accertamento penale*, Giuffrè, Milano, 2010;

MARAFIOTI L., *Digital evidence* e processo penale, in *Cass. pen*., 2011, pp. 4509-4523;

MARCHESE V., CAENAZZO L., RODRIGUEZ D., *Banca dati nazionale del Dna: bilanciamento tra diritti individuali e sicurezza pubblica nella legge 30 giugno 2009, n. 85*, in *Rivista Italiana di Diritto e Procedura Penale,* fasc.4, 2013, p. 1863;

MARCHETTI D., SOLECCHI G., CASCINI F., ALBERTACCI G., *Il valore probatorio dell'immagine digitale*, in *Giust. pen*., 2004, I, c. 276;

MARCOCCIO G., *Convention on Cybercrime: novità per la conservazione dei dati*, in *www.interlex.it*;

MARCOLINI S., *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen*., 2/2015, pp. 761.

MARCOLINI S., *Regole di esclusione e nuove tecnologie*, in *Criminalia*, 1/2006;

MARINO G., *Individuazione e prelievo di reperti utili per la ricerca del DNA: la Costituzione impone il contraddittorio?*, in *Diritto & Giustizia*, fasc.183, 2017, p. 6;

MARTURANO A., *Il corpo Digitale: natura, informazione, merce*, Giappichelli, Torino, 2010;

MASON S., *Electronic Evidence: Disclosure, Discovery and Admissibility*, LexisNexis, Londra, 2007;

MASSA T., *Le Sezioni unite davanti a "nuvole e orologi": osservazioni sparse intorno al principio di causalità*, in *Cass. pen*., 2002, p. 3643;

MASTROPAOLO F., *Prelievi del sangue a scopo probatorio e poteri del giudice*, in *Riv. it. Med. leg*., 9, 1987, pp. 1081;

MATHER K., *Elementi di biometria*, in *Testi e manuali per la scienza contemporanea. Serie di biologia e medicina*, Boringheri, Torino 1972;

MATTIUCCI M., DELFINIS G., *Forensic Computing*, in *Rassegna dell'Arma dei Carabinieri*, 2, 2006. p. 51 e ss.;

MAZZA O., *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *DPC Riv. Trim*, 3/2019;

MAZZACUVA N., PAPPALARDO G., *Prelievo ematico coattivo e accertamento della verità: spunti problematici*, in *Foro it*., 1987, I, 717 ss.

MCCARTNEY C., *The Dna expansion programme and criminal investigation*, in *Brit, J. Criminol*., 46, 2006, pp. 175-192;

MCEWAN I., *Macchine come me*, Einaudi, Torino, 2019;

MECHAM L. R., *Il sistema giudiziario federale negli Stati Uniti. Elementi introduttivi per i magistrati e gli amministratori giudiziari in altri paesi*, Washington D.C. 20544, 2001, disponibile su http://pub.raffaelecassia.it/sss/eclipse/legal_usa.pdf;

MELCHIONDA A., *voce "Prova in generale (dir. proc. pen.)"*, in *Enc. Dir*. XXXVIII, Torino, 1988;

MENDOLA M., *Aspetti informatici delle prove biometriche. Il problema dei "falsi positivi"*, in *Psicologia e Giustizia,* Anno 14, numero 1, Gennaio - Giugno 2013;

MENNA M., *La prova tra processo, scienza e verità. Quel rapporto giudice accertamento*, in *D&G*, 2006, f. 19, p. 95;

MEUWLY D., BAKER N., *Biometrics in the aliens' identity chain. A literature study final report* (WODC PROJECT 2965), reperibile all'indirizzo https://repository.wodc.nl/bitstream/handle/20.500.12832/2428/2965_volledige_tekst_tcm28-442367.pdf?sequence=3&isAllowed=y;

MEUWLY D., RAMOS D., HARAKSIM R., *A guideline for the validation of likelihood ratio methods used for forensic evidence evaluation*, in *Forensic Science International*, 276 (2017), pp. 142–153;

MILANI S., FONTANI M., BESTAGINI P., BARNI M., PIVA A., TAGLIASACCHI M., TUBARO S., *An overview on video forensic*, in *APSIPA Transactions on Signal and Information Processing*, vol. 1, (2012);

MILLER T., *Explanation in Artificial Intelligence: Insights from the social sciences*, in *Artif. Intell*., 2018, 267, pp. 1-38;

MIRAGLIA M., *Il IV Emendamento alla rincorsa del progresso: perquisizioni e lotta alla droga nel diritto Usa*, in *Dir. pen. proc*., 2002, 105 ss.;

MIRAGLIA M., *La ricerca della verità per condannare ed assolvere: il test del Dna e l'esperienza statunitense*, in *Dir. Pen. e Processo*, 2003, 12, 1555;

MITTELSTADT B., FLORIDI L., *The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts*, in *Science and Engineering Ethics 2016*, 22, pp. 303 ss.;

MITTONE A., *Libero convincimento e sapere scientifico: riflessioni sulla perizia nel processo penale*, in *Quest. giust*., 1983;

MNOOKIN J. L., *The validity of latent fingerprint identification: confessions of a fingerprinting moderate*, in *Law, Probability and Risk*, 2008, 7, pp. 127−141, si veda, https://lpr.oxfordjournals.org/content/7/2/127.full.pdf;

MOBILIO G., *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021;

MOENSSENS A. A., MEAGHER S. B., *Fingerprints and the law*, disponibile su http://www.crime-scene-investigator.net/fingerprintsourcebkchp13.pdf;

MOLINARI F. M., *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen*., fasc.3, 2013, p. 1259B;

MOLINARI F.M., *Le attività investigative inerenti la prova digitale*, in *Cass. pen.*, 3/2019, p. 1261;

MONATERI, P.G., *Diritti senza tempo né spazio*, in *Sole24ore*, 23.12.2012;

MONTECCHI G., VENUDA F., *Manuale di biblioteconomia*, Milano, Editrice Bibliografica, 1999;

MONTELEONE A., *Rilevazioni biometriche : lo stato della "privacy" delle "networked persons" tra il nuovo Codice ed i provvedimenti del Garante italiano*, in *Diritto&Diritti*, giugno 2004;

MONTESANO L., *Le "prove atipiche" nelle presunzioni e negli "argomenti" del giudizio civile*, in *Riv. dir. proc*., 1980, p. 246;

MORDINI E., *Il Volto e il Nome. Implicazioni Etiche, Sociali e Antropologiche delle Tecniche di Identificazione Biometriche*, in *MEDIC*, 2006, 14, pp. 29-40;

MORDINI E., OTTOLINI C., *Implicazioni etiche e sociali della biometria*, in *L'Arco di Giano*, 2005, n. 45, 67;

MORDINI E., PETRINI C., *Ethical and social implications of biometric identification technology*, in *Ann Ist Super Sanità* 2007 | Vol. 43, No. 1: 5-11;

MORELLI F., *Accertamenti e rilievi non ripetibili: una disciplina forse non incostituzionale, e tuttavia da rivisitare profondamente*, in *Giurisprudenza Costituzionale*, fasc.6, 2017, p. 2468C;

MORRISON G.S., *Consensus on validation of forensic voice comparison*, in *Science & Justice*, Volume 61, Issue 3, 2021, pp. 299-309;

MURA A., *Teorema di Bayes e valutazione della prova*, in *Cass. pen*., 2004, p.1814;

MUSSO R. G., *Il processo penale statunitense. Soggetti ed atti*, Giappichelli, Torino, 2001;

NAGEL E., *La struttura della scienza*, Iva ed., Milano, 1984;

NAIMOLI C., *Principio di falsificazione tra prova indiziaria e prova scientifica: riflessioni sul caso Garlasco e M. Kercher*, Ospedaletto, Pisa, Pacini giuridica, 2017;

NANAVATI S., THIEME M., NANAVATI R., *Biometrics. Identity verification in a networked world*, in *Wiley Computer Publishing*, 2002, 13-14;

NAPPI A., *Guida al codice di procedura penale*, 9° ed., Giuffrè, Milano, 2004;

NAPPI A., *Il prelievo ematico tra esigenza probatoria di accertamento del reato e garanzia costituzionale della libertà personale. Note a margine di un mancato bilanciamento tra valori*, in *Giur. cost*., 1996, p. 2151;

NAPPI A., *Libertà e legalità della prova in età moderna e contemporanea*, in *Cass. pen*., 2012, pp. 408 e ss.;

NEGRI D., *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Rivista italiana di diritto e procedura penale*, Vol. 63, 1, 2020;

NERONI REZENDE I., *Facial recognition in police hands: Assessing the "Claerview case" from a European perspective*, in *NJECL*, 2020, vol. 11, n. 3, p. 375 ss;

NEWTON D.E., *Dna Evidence and Forensic Science*, Infobase, New York, 2008;

NICOLICCHIA F., *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Wolter Kluwer, Milano, 2020;

NICOLICCHIA F., *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Diritto penale contemporaneo*, 2, 2018;

NIEVA-FENOLL J., *Intelligenza artificiale e processo*, (trad. a cura di) P. Comoglio, Giappichelli, Torino, 2019;

NOBILI M., *Art. 188 c.p.p.*, in AA.VV., *Commento al nuovo codice di procedura penale*, (a cura di) M. Chiavario, II, Utet, Torino, 1990, 396 s.;

NOBILI M., *Concetto di prova e regime di utilizzazione degli atti nel nuovo codice di procedura penale*, in *Foro it.*, 1989, c. 274;

NOBILI M., *Il diritto delle prove ed un rinnovato concetto di prova*, in AA. VV., *Commento al nuovo codice di procedura penale*, (a cura di) M. Chiavario, vol. II, Torino, 1990;

NOBILI M., *Il nuovo 'diritto delle prove' ed un rinnovato concetto di prova*, in *Leg. pen.*, 1989, pp. 395 e ss.;

NOBILI M., *La nuova procedura penale. Lezioni agli studenti*, CLUEB, Bologna, 1989;

NOBILI M., *Scenari e trasformazioni del processo penale*, Cedam, Padova, 1998;

NOBILI M., *Storie d'una illustre formula: il "libero convincimento" negli ultimi trent'anni*, in *Riv. it. dir. proc. pen.*, 2003.

NOBILI M., *sub art. 189* c.p.p., in AA. VV., *Commento al nuovo codice di procedura penale*, (a cura di) M. Chiavario, vol. II, Torino, 1990;

NOBILI M., *sub art. 191* c.p.p., in AA. VV., *Commento al nuovo codice di procedura penale*, (a cura di) M. Chiavario, vol. II, Torino, 1990;

NOBILI M., *sub art. 192* c.p.p., in AA. VV., *Commento al nuovo codice di procedura penale*, (a cura di) M. Chiavario, vol. II, Torino, 1990;

NOFRI M., *Obbligatorio l'esame dibattimentale del perito già escusso in sede di incidente probatorio ex art. 392 comma 2 c.p.p.*, in *Giur. it.*, 1999, c. 383;

NUNIN R., *Utilizzo dei dati biometrici da parte del datore di lavoro: la prescrizione del Garante per la privacy*, in *Il lavoro nella giurisprudenza*, 2007, 2;

NUNZIATI M., *Note sul riconoscimento del parlante*, in http://www.teutas.it/societa-informazione/prova-elettronica/381-note-sul-riconoscimento-del-parlante.html.;

OATLEY G., EWART B., *Data mining and crime analysis*, in *Wiley Interdisciplinary Reviews (WIREs): Data Minining and Knowledge Discovery* 1(2), pp. 147–153;

ORLANDI R., PAPPALARDO G., *L'indagine genetica nel processo penale germanico: osservazioni su una recente riforma*, in *Dir. pen. proc.*, 1999, 764;

ORLANDI R., *Atti e informazioni dell'autorità amministrativa nel processo penale: contributo allo studio delle prove extracostituite*, Giuffrè, Milano, 1992;

ORLANDI R., PAPPALARDO G., *L'indagine genetica nel processo penale germanico: osservazioni su una recente riforma*, in *Dir. pen, proc.*, 1999, pp. 762 e ss.;

PACE A., *voce Libertà personale (diritto costituzionale)*, in *Enc. Dir.*, Vol. XXIV, Giuffrè, Milano;

PAGALLO U., *Intelligenza Artificiale e diritto. Linee guida per un oculato intervento normativo*, in *Sistemi intelligenti*, 3, 2017, 615 ss;

PAGALLO U., *Introduzione alla fisolofia digitale. Da Leibniz a Chaitin*, Giappichelli, Torino, 2005;

PAGALLO, U., *La tutela della privacy negli Stati Uniti d'America e in Europa. Modelli giuridici a confronto*, Giuffrè, Milano, 2008;

PALERMO G. B., MASTRONARDI V., AGOSTINI S., *Il processo investigativo e accusatorio negli Stati Uniti d'America e in Italia*, in *Supplemento alla Rivista di psichiatria*, 2012, 47,4, pp. 42S- 45S;

PALIOTTA A.P., *Le politiche innovative di sicurezza nelle città tra tecnologie di riconoscimento* e *smart cities*, in *SINAPPSI - Connessioni tra ricerca e politiche pubbliche* | Anno X | n. 2/2020;

PALMIOTTO F., *Le indagini informatiche e la tutela della riservatezza informatica*, in *www.lalegislazionepenale.it*, 1.7.2019;

PANZAVOLTA M., *I profili dell'istituto*, in *Giur. it*., 2010, p. 1222;

PANZAVOLTA M., *Legalità e proporzionalità nel diritto processuale penale*, in AA.VV., *Carta dei diritti fondamentali dell'Unione europea*, (a cura di) R. Mastroianni, O. Pollicino, S. Allegrezza, O. Razzolini, F. Pappalardo, Giuffrè, Milano, 2017;

PAOLONI A., *Identificazione personale in ambito forense*, in *Mondo Digitale*, Settembre 2014, p. 6;

PAOLONI A., *La voce come elemento di identificazione della persona*, in AA.VV., *La voce come bene culturale*, (a cura di) A. De Dominicis, Carocci, Roma, 2002;

PAOLUCCI F., *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *Medialaws*, 1/2021;

PARK U., TONG Y., JAIN A.K., *Age-invariant face recognition*, in *IEEE Trans. Pattern Anal. Mach. Intell*., vol. 32, no. 5, pp. 947954, May 2010;

PARODI C., SELLAROLI V., *Sistema penale e intelligenza artificiale: molte esperienze e qualche equivoco*, in *www.dirittopenalecontemporaneo.it*, 6/2019;

PASCUCCI N., La natura controversa della ricognizione fotografica, in *RIDPP* fasc.1, 2017;

PASQUALE F., *The Black Box Society: The Secret Algorithms that Control Money and Information*, Cambridge, London, 2015;

PASQUINUCCI A., *Biometria e Sicurezza informatica*, in *ICT Security* n. 39-40-41-42, Novembre 2005 – Febbraio 2006, si veda http://www.ucci.it/docs/ICTSecurity-2006-42.pdf;

PASSAIN M., *La privacy è morta, viva la privacy. Tutti i modi in cui veniamo controllati, spiati, schedati. Tutto quello che occorre sapere per difendersi*, Adriano Salani Editore, Firenze, 2009;

PATANÈ V., *Il diritto al silenzio dell'imputato*, Giappichelli, Torino, 2006;

PATO J. N., MILLETT L. I. (eds.), *Biometric Recognition: Challenges and Opportunities*, in *The National Academies Press* at http://www.nap.edu/catalog.php?record_id=12720;

PERFETTI T., *Biometria tra privacy e sicurezza*, in *www.computerlaw.it*;

PERRI P., *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè, Milano, 2020;

PETERSON G., SHENOI S., *Advances in Digital Forensics*, Springer, Orlando, 2009;

PEZZUTO R., *Accesso transazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione Europea al vaglio del Consiglio dell'Unione*, in *Dir. Pen. cont*, fasc. 2/2019, pp. 80 e ss.;

PICCOTTI L., *La ratifica della Convenzione del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir.pen.proc*., 2008, 700;

PICOZZI M., INTINI A., *Scienze forensi. Teoria e prassi dell'investigazione scientifica*, Utet, Torino, 2009;

PISAPIA G. D., *voce Errore giudiziario (riparazione dell'), II) Dir. proc. Pen.*, in *Enc. Giur*., vol. XIII, Roma, 1989, 2;

PITTIRUTI M., *Digital evidence e procedimento penale*, Giappichelli, Torino, 2017;

PIVATY A., *Suspects' privilege against self-incrimination not violated when made to unlock smartphone with fingerprint, Dutch Supreme Court rules*, in *Fair Trials*, 19 febbraio 2021;

PIZZI C., *Abduzione e serendipità nella scienza e nel diritto*, in *Cass. pen*., 2005, pp. 234 e ss.;

POISSON S.D., *Recherches sur la probabilitè des jugements en matière criminelle et en matière civile*, Imprimeur – libraire, Parigi, 1837;

POLIDORO D., *Tecnologie informatiche e procedimento penale: la giustizia penale messa alla prova dall'intelligenza artificiale*, in *Arch. Pen*., fasc. 3, 2020 (Web);

PONZANELLI G., *Scienza, verità e diritto: il caso Bendectin*, in *Foro it*., 1994, IV, c. 184;

POPPER K.R., *Logica della scoperta scientifica*, Einaudi, Torino, 1970;

POPPER K.R., *Scienza e filosofia*, Einaudi, Torino, 1969;

POTETTI D., *Art. 228 comma 3 c.p.p.: il "perito istruttore"*, in *Cass. pen*., 1997, p. 1544;

PREITE G., *Il riconoscimento Biometrico: Sicurezza vs. Privacy*, UNI Service, Trento, 2008;

PREITE, G., *Politica e biometria. Nuove prospettive filosofiche delle scienze sociali*, Tangran edizioni scientifiche, Trento, 2016;

PRESUTTI A., *L'acquisizione forzosa dei dati genetici tra adempimenti internazionali e impegni costituzionali*, in *Rivista italiana di diritto e procedura penale*, 2010, Vol. 53, fasc. 2, pp. 547-559;

PRETTI D., *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni*, in *www.sistemapenale.it*, 2020, 71 ss;

PRETTI D., *Prime riflessioni a margine della nuova disciplina delle intercettazioni*, in *www.dirittopenalecontemporaneo.it*, 2018, (1), 189 ss.;

PRINS C., *Biometric Technology Law, Making Our Body Identify for us: Legal Implications of Biometric Technologies*, (1998) 14(3) in *Computer Law and Security Report 159*, p. 163;

PULICE M., *Sistemi di rilevazione di dati biometrici e privacy*, in *Lavoro nella Giurisprudenza*, 2009, 10, 994;

PULITANÒ D., *Il diritto penale fra vincoli di realtà e sapere scientifico*, in *Riv. it. dir. proc. pen*., 2006, 802 ss.;

PULITO L., *Il trattamento dei dati personali in ambito penale e l'uso del passenger name record per contrastare il terrorismo e altri reati gravi*, in *Processo penale e giustizia*, 2018, 6, p. 1148;

PUTIGNANO D. S.*, L'errore scientifico nel processo penale. Rilievi pratici e riscontri giurisprudenziali*, Giuffrè, Milano, 2007;

QUATTROCOLO S., ANGLANO C., CANONICO M., GUAZZONE M., *Techical Solutions for Legal Challenges: Equality of Arms in Criminal proceeding*, in *Global Jurist*, vol. 20, no. 1, 2020;

QUATTROCOLO S., *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, 2020;

QUATTROCOLO S., *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Rev. Italo-espanola derecho procesal*, 2019, 1;

QUATTROCOLO S., *Equo processo e sfide della società algoritmica*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2019, pp. 135-144;

QUATTROCOLO S., *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali ed informatiche*, in *www.lalegislazionepenale.it*, 18 dicembre 2018;

QUATTROCOLO S., *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, Saggi - Focus: innovazione, diritto e tecnologia: temi per il presente e il futuro, pp. 121 ss.;

QUATTROCOLO S., *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, in *Cass. pen*., 4/2019, pp. 1748-1765;

KOSTORIS R.E., *Alt ai prelievi di sangue coattivi*, in *Dir. pen. e proc*., 1996, p. 109 e ss.;

RAFARACI T., *Ricognizione informale dell'imputato e (pretesa) fungibilità delle forme probatorie*, in *Cass. pen*., 1998, p. 1741;

RAMAIOLI S., *Rilievi dattiloscopici: aspetti medico-legali ed efficacia probatoria*, in *Mass. ann. Cass. pen*., 1980, p. 1143;

RAMEN R.V., YAMPOOLSKIY V., *Biometrics: a survey and classification*, in *Biometrics*, vol. 11, no. 1, 2008;

RANALDI G., *Processo penale e prova informatica: profili introduttivi*, in *Diritto Pubblico Europeo online* n. 2/2020;

RATHA N.K., CONNELL J.H., BOLLE R.M., *Enhancing security and privacy in biometrics-based authentication systems*, in *IBM Systems Journal* 40(3), 614–634 (2001);

REITH M., CARR C.N., GUNSH G., *An Examination of Digital Forensic Models*, in *International Journal of Digital Evidence*, OH, Fall 2002, Vol.1, Issue 3, pp. 6-7. Si v. http://www.ijde.org;

RENZETTI S., *La prova scientifica nel processo penale: problemi e prospettive*, in *Rivista di Diritto Processuale*, 2/2015;

RESTA F., *La disciplina acquista maggiore organicità per rispondere alle esigenze applicative*, in *Guida al dir*., 2008, f. 16;

RESTA F., POLLICINO O., *Riconoscimento facciale e protezione dati: attenzione al punto di non ritorno*, in *Diritti Comparati – Comparare i diritti fondamentali in Europa*, 30.1.2020;

REUBEN M., MORLEY J., *Investigation into the use of photoanthropometry in facial image comparison*, in *Forensic science international*, 212.1 (2011), pp. 231-237;

RICCI A., *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati. Riflessioni sul d.lgs. 18 maggio 2018, n. 51, di attuazione della dir. 2016/680/UE*, in *Le Nuove leggi civili commentate*, 3, 2019, 565 ss.;

RICCI R., *La prova del DNA per la ricerca della verità: aspetti giuridici, biologici e probabilistici*, Giuffrè, Milano, 2006;

RICCI U., *Dna e crimine: dalla traccia biologica all'identificazione genetica*, Laurus Robuffo, Roma, pp. 108 e ss.;

RICCI U., *L'accreditamento ISO 17025:2005 nel laboratorio di genetica forense*, in *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)*, fasc. 1, 2014, p. 69;

RICCI U., *La qualità nel settore della genetica forense*, in *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)*, fasc. 1, 2016, p. 233;

RICCI U., PREVIDERÈ C., FATTORINI P., CORRADI F., *La prova del Dna per la ricerca della verità. Aspetti giuridici, biologici e probabilistici*, Giuffrè, Milano, 2006;

RICCI U., *Un lampo di consapevolezza nella normativa italiana: il DNA oltre la suggestione e il mito*, in *Diritto penale e processo*, 6/2016, pp. 751 e ss.;

RICCIO G., *Ragionando su intelligenza artificiale e processo penale*, in *Arch. pen*., fasc. n. 3, 2019 (Web);

RIVELLO P., *Tecniche scientifiche e processo penale*, in *Cass. pen*., Fasc. 4, 2013, p. 1691 e ss.;

RIVELLO P.P., *Il processo e la scienza*, in *Riv. it. dir. e proc. pen*., fasc.4, 2010, p. 1715;

RIVELLO P.P., *voce Perito e perizia*, in *Dig. disc. pen*., vol. IX, Torino, 1995, pp. 478 e ss.;

ROBERTS D.E., *Collateral Consequences, Genetic Surveillance, and the New Biopolitics of Race*, University of Pennsylvania Law School, Pennysylvania, 2011;

RODOTÀ S., *Dal soggetto alla persona*, Editoriale Scientifica, Napoli, 2007;

RODOTÀ S., *Il diritto di avere diritti*, Laterza, Roma 2012, p. 319;

RODOTà S., *Ipotesi sul corpo "giuridificato"*, in *Tecnologie e diritti*, Bologna, 1995, 204;

RODOTÀ S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica del diritto privato*, 4, 1997, p. 606;

RODOTÀ S., *Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, all'indirizzo https://www.privacy.it/archivio/rodo20040916.html;

RODOTà S., *Tecnologie e diritti*, Il Mulino, Bologna, 1995;

RODOTÀ S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997;

ROMANO M., *Commentario sistematico del codice penale*, vol. I, Milano, 2004.

ROSANÒ A., *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'unione europea: le proposte della commissione europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence)*, in *www.lalegislazionepenale.it*, 16.10.2020;

ROSS A., SHAH J. AND JAIN A.K., *From Template to Image: Reconstructing Fingerprints From Minutiae Points*, in *IEEE Transactions on Pattern Analysis and Machine Intelligence, Special Issue on Biometrics*, Vol. 29, No. 4, pp. 544-560, April 2007;

ROSS A., SHAH J., JAIN A., *From Template to Image: Reconstructing Fingerprints from Minutiae Points, (2007) 29(4)*, in *IEEE Transactions on Patterns Analysis and Machine Intelligence*, p. 544;

RUFFOLO U., RICCIO G., URICCHIO A.F., *Intelligenza Artificiale tra etica e diritti*, Cacucci ed., Bari, 2020;

RUGANI G., *La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della direttiva (UE) 2016/680: frammentazione ed incertezze applicative*, in *Freedom, Security & Justice: European Legal Studies Rivista quadrimestrale on line sullo Spazio europeo di libertà, sicurezza e giustizia* 2019, n. 1, p. 87;

RULLI E., *Giustizia predittiva, intelligenza artificiale e modelli probabilistici. Chi ha paura degli algoritmi?*, in *Il Mulino Rivisteweb, Analisi Giuridica dell'Economia*, Fascicolo 2, dicembre 2018;

SACCHETTO E., *Biometrics as forensic evidence: some reflections from the Italian Criminal proceeding's point of view*, in *8th International Workshop on Biometrics and Forensics (IWBF)*, 2020, pp. 1-4;

SACCHETTO E., *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *www.lalegislazionepenale.it*, 16.10.2020;

SACCHETTO E., *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2/2019;

SACKS M. J., KOEHLER J. J., *The Individualization Fallacy in Forensic Science Evidence*, 2/8/2008, pp. 219-220, disponibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1432516;

SALARDI S., *Dna ad uso forense: paladino di giustizia o reo di ingiustizie?*, in *Riv. it. medicina legale (dal 2012 Riv. it. medicina legale e dir. Sanitario)*, fasc. 6, 2011, p. 1359;

SANGUINETI, L., *La valutazione della prova*, Giuffè, Milano, 1979;

SANTOSUOSSO A., *Diritto, scienza, nuove tecnologie*, Cedam, Padova, 2016;

SANTOSUOSSO A., *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Mondadori, Milano, 2020;

SAPONARO L., *Dall'indizio alla prova indiziaria : il rapporto tra probabilità e certezza*, Wolters Kluwer, Padova, 2015;

SAPONARO L., *L'impatto processuale delle immagini: fotografie e videoriprese*, Wolters Kluwer, Milano, 2020;

SARTOR G., *Intelligenza artificiale e diritto. Un'introduzione*, Giuffrè, Milano, 1996;

SARZANA C., S. IPPOLITO, *Informatica, internet e diritto penale*, Giuffrè, Milano, 2010;

SARZANA C., *Evoluzione tecnologica e diritti dell'individuo*, in *Dir. Inf.*, 1992, pp. 393-411;

SCAFFARDI L., *Forensic genetics: The evolving challenge of DNA cross-border exchange*, in *BioLaw Journal –Rivista di BioDiritto*, Special Issue 1(2021), pp. 329 e ss.;

SCAFFARDI L., *Next Generation Prüm e le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, in *Federalismi.it*, 8, 2021, pp. 200 ss.;

SCAGLIARINI S., *La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio*, Aracne, Roma, 2013;

SCALFATI A. *Le indagini atipiche*, Torino, Giappichelli, 2014;

SCALFATI A., *Gli accertamenti tecnici dell'accusa*, in *Indice pen*., 1992;

SCALFATI A., *La deriva scientista dell'accertamento penale*, in *Proc. pen. giust*., 2011, 5, p. 144;

SCALFATI A., *Le indagini atipiche*, Giappichelli, Torino, 2014;

SCALFATI A., *Note minime su cooperazione investigativa e mutuo riconoscimento*, in *Proc. pen. giust.*, 2017, pp. 217 s.;

SCALFATI A., *voce Consulenza tecnica (dir. proc. pen.)*, in *Enc. giur*. Treccani, vol. VIII, Roma, 1997;

SCAPARONE M., *Elementi di procedura penale. I princìpi costituzionali*, Giuffrè, Milano, 1999;

SCAPARONE M., *Evoluzione e involuzione del diritto di difesa*, Giuffrè, Milano, 198;

SCAPARONE M., *Procedura penale*, 2 ed°, I, Giappichelli, Torino, 2010;

SCAPARONE M., *sub* art. 24 c. 2 Cost., in *Comm. Cost. Branca*, Bologna-Roma, 1981;

SCARCELLA A., *Conservazione delle impronte digitali degli "assolti" e violazione dell'art. 8 Conv.e.d.u.*, in *Dir. Pen. e Processo*, 2013, 7, 809;

SCARSCELLA A., *Condizioni dell'efficacia probatoria nell'indagine dattiloscopica*, in *Dir. Pen. e Processo*, 2012, 1, 68;

SCARSCELLA A., *Prelievo del Dna e banca dati nazionale*, Cedam, Padova, 2009;

SCHELLINO D., *Corte costituzionale e accertamenti peritali coattivi incidenti nella sfera corporale della persona*, in *Leg. Pen*., 1990 173 e ss.;

SCHWEITZER N. J., SACKS M. J., *The CSI effect: popular fiction about forensic science affects the public's expectations about real forensic science*, in *Jurimetrics J*., 47, 2007, p. 358, disponibile su: http://www.public.asu.edu/~nschwei/archive/csieffect.pdf;

SCIPIONE J., LO MONACO M., *Has the horse bolted? Dealing with legal and practical challenges of facial recognition*, in *Media Laws*, 18.1.2022;

SEAMAN J.A., *Black Boxes*, in *Emory Law Journal* 58, no. 2 (2008): pp. 427-488;

SECKINERA D., MALLETTA X.,B , ROUXA B.C., MEUWLY D., MAYNARDA P., *Forensic image analysis – CCTV distortion and artefacts*, in *Forensic Science International*, 285, 2018, pp. 77–85;

SHALEV-SHWARTZ S., BEN-DAVID S., *Understanding Machine Learning: From Theory to Algorithms*, Cambridge University Press, New York, 2014;

SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*. Giappichelli, Torino, 2018;

SIMONCINI A., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2019, pp. 63-88;

SINGH M., NAGPAL S., SINGH R., VATSA M., *On Recognizing face images with weight and age variations*, in *Proc. IEEE Digital Object Identifier*, vol. 2, 2014;

SIRACUSANO D., *Introduzione allo studio del processo penale*, Milano, 1989;

SIRACUSANO D., *Studio sulla prova delle esimenti*, Milano, 1959;

SIRACUSANO D., *voce Prova*, in *Enc. giur. Treccani*, vol. XXV, Roma, 1991;

SIRACUSANO F., *La prova informatica*, in *Associazione tra gli studiosi del processo penale "G.D. Pisapia", XXX Convegno Nazionale, Roma 20-21 ottobre 2016 – Università La Sapienza "Investigazioni e prove transnazionali"*;

SIRACUSANO F., *Tra semplificazione e ibridismo: insidie e aporie dell'Ordine europeo di indagine penale*, in *Arch. pen.*, 2017, n. 2;

SLOBOGIN A., *Public privacy: camera surveillance of public spaces*, 2002, pp. 219-223, consultabile su http://www.olemiss.edu/depts/ncjrl/pdf/LJournal02Slobog.pdf;

SMUHA N. ET AL., *How the Eu can achieve legally trustworthy AI: a response to the European Commission's Proposal for an Artificial Intelligence Act*, reperibile all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991 (visualizzato in data 22.2.2022);

SMUHA N.A., AHMED-RENGERS E., HARKENS A., LI W., MACLAREN J., PISELLI R., YEUNG K., *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, 2021, reperibile all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991 (visualizzato in data 20.2.2022);

SMYTH S., *Biometrics, surveillance and the law. Societies of restricted access, discipline and control*, Routledge, New York, 2019;

SORELL M., *Video provenance by motion vector analysis: A feasibility study*, in *International Symposium on Communications, Control, and Signal Processing* (ISCCSP), (2012);

SPAGNOLO P., *Il Tribunale della libertà. Tra normativa nazionale e normativa internazionale*, Giuffrè, Milano, 2008;

SPAGNOLO P., *La nuova cooperazione giudiziaria penale: mutuo riconoscimento e tutela dei diritti fondamentali*, in *Cass. pen*., fasc.3, 1.3.2020, p. 1290;

SPINELLA A., SOLLA G., *L'identificazione personale nell'investigazione scientifica: DNA e impronte*, in *Cass. pen*., 2009, 1, p. 428 ss.;

SPINNEY L., *The Fine Print*, in *Nature*, vol. 464/18 marzo 2010, 344;

STEFANINI E., *Dati genetici e diritti fondamentali*, Cedam Padova, 2008;

STELLA F., *Giustizia e modernità. La protezione dell'innocente e la tutela delle vittime*, 3° ed., Milano, 2003;

STELLA F., *Leggi scientifiche e spiegazione causale del diritto penale*, Giuffrè, Milano, 2000;

STONE M., *La cross-examination. Strategie e tecniche*, Milano, 1990;

STONEY D. A., *Measurement of Fingerprint Individuality*, in *Advances in Fingerprint Technology* 327, 329 (Henry C. Lee & Robert E. Gaensslen eds., 2d ed. 2001);

TAGLIARO F., D'ALONA E., SMITH F. P., *L'ammissibilità della prova scientifica in giudizio e il superamento del Frye standard: note sugli orientamenti negli Usa successivi al caso Daubert v. Merrel Down Pharmaceuticals, Inc.*, in *Riv. it. med. leg*., 2000, p. 719;

TALLACCHINI M., *Bodyright. Corpo biotecnolgico e diritto*, in *Biblioteca della libertà*, 1998, 21-50;

TALLACCHINI M., *Il corpo e le sue parti. L'allocazione giuridica dei materiali biologici umani*, in *Medicina e Morale*, 1998, pp. 499-544;

TALLACCHINI M., *Retorica dell'anonimia e proprietà dei materiali biologici umani*, in AA.VV., *Corpo esibito, corpo violato, corpo venduto, corpo donato. Nuove forme di rilevanza giuridica del corpo umano*, (a cura di) F. D'Agostino, Milano, Giuffrè, 2003, 171-192;

TARUFFO M., *Certezza e probabilità nelle presunzioni*, in *Il foro italiano*, 1974, p. 83;

TARUFFO M., *Il diritto alla prova nel processo civile*, in *Riv. dir. proc*., 1984, p. 77;

TARUFFO M., *Judicial decision and Artificial Intelligence*, in *Artificial Intelligence and Law*, 1998, pp. 311 e ss.;

TARUFFO M., *La prova dei fatti giuridici. Nozioni generali*, Giuffrè, Milano, 1992;

TARUFFO M., *Modelli di prova e di procedimento probatorio*, in *Riv. dir. proc*., 1990, p. 420;

TARUFFO, M., *La prova dei fatti giuridici. Nozioni generali*, Giuffrè, Milano, 1992;

TASPINAR M., NASKALI A. T., EREN G., KURT M., *The importance of customized advertisement delivery using 3D tracking and facial recognition*, in *2012 Second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP)*, 2012, pp. 520-524;

TAULLI T., *Artificial Intelligence Basics*, Apress, Berkeley, 2019;

TERRACIANO U., *La metodologia dell'investigazione*, Franco Angeli, Milano, 2014;

TESTAGUZZA, A., *Digital Forensics. Informatica giuridica e processo penale*, Cedam, Milano, 2014;

THOMPSON W. C., TARONI F., AITKEN C.G.G., *How the probability of a False Positive Affects the Value of Dna Evidence*, in *J. Forensic Science*, Jan. 2003, Vol. 48, No. 1, pp. 1-2;

TONINI P., *Accertamento del fatto e informazioni genetiche: un difficile bilanciamento*, in *Dir. pen. proc.*, 2009, Dossier: Banca dati nazionale del DNA e prelievo di materiale biologico, p. 3;

TONINI P., CONTI C., *Il diritto delle prove penali*, Giuffrè, Milano, 2012;

TONINI P., *Documento informatico e giusto processo*, in *Dir. pen. proc*., 2009, p. 403;

TONINI P., *Il contraddittorio: diritto individuale e metodo di accertamento*, in *Dir. pen. proc*., 2000, p. 1388;

TONINI P., *Il valore probatorio dei documenti contenenti dichiarazioni scritte*, in *Cass. pen*., 1990, p. 2212;

TONINI P., *La Cassazione accoglie i criteri Daubert sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza*, in *Diritto penale e processo*, 11, 2011, 1341 ss.;

TONINI P., *La prova penale*, Cedam, Padova, 2000;

TONINI P., *La prova scientifica: considerazioni introduttive*, in *Dir. pen. proc*., 2008, n. 6, Dossier La prova scientifica nel processo penale;

TONINI P., *Manuale di procedura penale*, Giuffrè, Milano, 2019;

TONINI P., *Problemi insoluti della prova documentale*, in *Dir. pen. proc*., 1996;

TONINI, P. *Prova scientifica e contraddittorio*, in *Diritto penale e processo*, 2003, p. 1459 ss.;

TORRE M., *Privacy e indagini penali*, Giuffrè, Milano, 2020;

TOSI O., *Voice identification. Teory and Legal applications*, University Park Press, Baltimora, 1979;

TRAVERSI A., *Intelligenza artificiale applicata alla giustizia: ci sarà un giudice robot?*, in *www.questionegiustizia.it.*;

TRAVERSO F., *Il diritto alla controprova nei rapporti con la perizia*, in *Dir. pen. proc*., 1998, p. 596;

TRINGALLI G., *Banche dati di Polizia: sussiste il diritto alla privacy e all'oblio?*, 24 settembre 2014, disponibile su http://www.altalex.com/documents/news/2014/10/10/banche-dati-di-polizia-sussiste-il-diritto-alla-privacy-e-all-oblio;

TROISI P., *L'errore giudiziario tra garanzie costituzionale e sistema processuale*, Cedam, Padova, 2011;

TSAMADOS A., AGGARWAL N. COWLS J. ET AL., *The ethics of algorithms: key problems and solutions*, in *AI & Soc* 37, 2022, pp. 215–230;

TURING A., *Intelligenza meccanica*, Bollati Boringhieri, Torino, 1994;

UBERTIS G., *Considerazioni generali su investigazioni e prove transnazionali*, in *Cass. pen*., 2017, 1, 50;

UBERTIS G., *Fatto e valore nel sistema probatorio penale*, Giuffrè, Milano, 1979;

UBERTIS G., *La conoscenza del fatto nel processo penale*, Giuffrè, Milano, 1992;

UBERTIS G., *La prova penale. Profili giuridici ed epistemologici*, Giappichelli, Torino, 1995;

UBERTIS G., *La tutela del contraddittorio e del diritto di difesa tra CEDU e Trattato di Lisbona*, in, *Cass. pen.*, 2010, p. 2494;

UBERTIS G., *Profili di epistemologia giudiziaria*, Giuffrè, Milano, 2015;

UBERTIS G., *Sistema di procedura penale*, Giappichelli, Torino, 2004;

UBERTIS G., *voce Giusto processo (diritto processuale penale)*, in *Enc. dir., Annali*, vol. II, t. 1, Milano, 2008;

UBERTIS, G., *Il giudice, la scienza, la prova*, in *Cass. pen.*, 2011, p. 4112 ss.;

VACIAGO G., *Digital Evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli, Torino, 2012;

VALLI R., *Le indagini scientifiche nel procedimento penale*, Giuffrè, Milano, 2013;

VAN DER PLOEG I., *The Politics of Biometric Identification. Normative aspects of automated social categorization*, in *www.biteproject.org/documents/politics_of_biometric_identity%20.pdf*.;

VAN DER PLOG I., *Biometric identification technologies: ethical implications of the information of the body. Biometric Technology & Ethics*, in *BITE Policy* Paper, no. 1, 2005;

VAN DIJK P., VAN HOOF G.H.J., T*heory and Practice of the European Convention on Human Rights*, 3rd ed., Martinus Nijoff, Leiden, 1998, p. 430 ss.;

VAN NATTA M. ET AL., *The rise and regulation of thermal facial recognition technology during the Covid-19 pandemic*, in *Journal of Law and the Biosciences*, 7, 1, gennaio-giugno 2020;

VASSALLI G., *Il diritto alla libertà morale (Contributo alla teoria dei diritti della personalità)*, in *Studi in memoria di Filippo Vassalli*, II, UTET, Torino, 1960, 1629 ss.;

VASSALLI G., *Il diritto alla prova nel processo penale*, in *Riv. it. dir. proc. pen.*, 1968, pp. 2 e ss.;

VECCHIO F., *Le intercettazioni da remoto e i diversi modelli di bilanciamento tra esigenze investigative e diritto alla riservatezza e all'integrità dei sistemi informatici*, in *La Cittadinanza europea*, 1/2016, pp. 107-127;

VERSTA L.G., *Voiceprint identification*, Nature, New York, 1962.;

VICOLI D., *Riflessioni sulla prova scientifica: regole inferenziali, rapporti con il sapere comune, criteri di affidabilità*, in *Riv. it. med. leg.*, 2013, p. 1239 ss;

VIGONI D., *Corte costituzionale, prelievo ematico coattivo e test del Dna*, in *Riv. it. dir. e proc. pen.*, fasc.4, 1996, p. 1022;

VIOLA P., JONES M., *Rapid Object Detection Using a Boosted Cascade of Simple Features*, in *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2001, 511 ss;

VOENA G.P., *(voce) Difesa: III) difesa penale*, in *Enc. Treccani*, Roma, 1989;

WACHTER S., MITTELSTADT B., FLORIDI L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017;

WALTL B., VOGL R., *Explainable Artificial Intelligence – the New Frontier in Legal Informatics*, in *Jusletter* IT, 22.2.2018;

WANG W., *Il manuale del giovane hacker*, Tecniche nuove, Milano, 2006;

WARREN S. D. - BRANDEIS L. D., *The right of privacy*, in 4 *Harvard Law Review* 193 (1890);

WATCHER S., MITTLESTADT B., FLORIDI L., *Why a right to explanation of automated decision-making does not exist in the GDPR*, in *International Data Privacy Law*, vol. 7, 2017, pp. 76 ss;

WAYMAN J., JAIN A., MALTONI D., MAIO D., *Biometric Systems. Techonology, Design and Perfomance Evaluation*, Springer, London, 2005;

WAYMAN J. L., *The History of Information Security: A Comprehensive Handbook*. Elsevier, Amsterdam, 2007;

WAYMAN J., MCIVER R., WAGGETT P., CLARKE S., MIZOGUCHI M., BUSCH C., DELVAUX N., ZUDENKOV A., *Vocabulary harmonisation for biometrics: the development of ISO/IEC 2382 Part 37*, in *The Institution of Engineering and Technology*, Vol. 3, 1, March 2014, p. 1 – 8;

WAYMAN J.L., *Fundamentals of biometric authentication technologies*, in *Int. J. Image Graphics*, vol. 1, no. 1, pp. 93–113, 2001;

WAYMAN J.L., *Fundamentals of biometric authentication technology*, in *Proceedings cardtech/securtech*, Chicago, 11–14 may 1999;

WAYMAN, J. L. (2000), a *Definition of "Biometrics"*, in National Biometric Test Center Collected Works, San Jose State University, 2000;

WEST E. M., *Court Findings of Prosecutorial Misconduct Claims in Post-Conviction Appeals and Civil Suits Among the First 255 Dna Exoneration Cases*, 2010, disponibile su https://www.nacdl.org/WorkArea/DownloadAsset.aspx?id;

WOODS T.P., *The Implicit Bias of the Implicit Bias Theory*, in *Drexel Law Review*, 2017, pp. 631 e ss.;

WOODWARD J. D., HORN C., GATUNE J., THOMAS A., *Biometrics A Look at Facial Recognition in Public Safety and Justice*, RAND, 2003;

WOODWARD J. D., ORLANS N. M., HIGGINGS P. T., *Identity Biometrics*, McGraw-Hill, 2003;

ZACCHÈ F., *La prova documentale*, Giuffrè, Milano, 2012;

ZALNIERIUTE M., *Burning Bridges: the automated facial recognition technology and public space surveillance in the modern State*, in *Colum. Sci. & Tech. L. Rev*., Vol. 22, pp. 284 e ss.;

ZAPPALÀ E. , *Il principio di tassatività dei mezzi di prova nel processo penale*, Giuffrè, Milano, 1982;

ZATIKO K., *Commentary: Defining digital forensics*, in *Forensic Magazine*, 2007, disponibile al seguente URL: http://www.forensicmag.com/node/128;

ZAVRSNIK A., *Criminal justice, artificial intelligence systems and human rights*, in *ERA Forum* (2020);

ZENCOVICH Z. V., *voce "Identità personale"*, nel *Digesto IV ed., Disc. priv., sez. civ.*, IX, Utet, 1993, 294-303;

ZICCARDI G., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, Milano, 2015;

ZICCARDI G., *L'avvocato hacker. Informatica giuridica e uso consapevole (e responsabile) delle tecnologie*, Giuffrè, Milano, 2012;

ZICCARDI G., *Scienze forensi e tecnologie informatiche: la computer and network forensics*, in *Informatica e diritto*, Vol. XV, 2006, n. 2, pp. 103-125;

ZIOSI M., HEWITT B., JUNEJA P., TADDEO M., FLORIDI L., *Smart Cities: Mapping their Ethical Implications*, 5.1.2022, reperibile all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4001761;

ZIROLDI A., *Intelligenza artificiale e processo penale tra norme, prassi e prospettive*, in *Questione Giustizia*, 18.10.2019;

ZUBOFF S., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Roma, 2019;

ZUCCONI V., *Pena di morte, la svolta dell'FBI*, La Repubblica, 12/1/2006.