Informatica e diritto, XLII annata, Vol. XXV, 2016, n. 1, pp. 29-45

Droni, privacy e tutela dei dati personali

LARA MERLA*

SOMMARIO: *1. Introduzione – 2. Livelli d'astrazione – 2.1. Il diritto come meta-tecnologia – 2.2. Il* design *della privacy – 3. Tra Stati Uniti e Unione europea – 4. Tra Unione europea e Italia – 5. Conclusioni*

1. INTRODUZIONE

Uno dei settori della ricerca contemporanea più ricco di finanziamenti è certamente la robotica, soprattutto militare. Al suo interno, un notevole spazio è occupato dall'ambito della progettazione e produzione di RPAs - *Remotely Piloted Aircrafts*, UAS - *Unmanned Aircraft System* o più semplicemente "droni", settore che gode di una particolare fortuna (non solo economica). Gli investimenti sono in continua crescita. Uno studio di mercato del gruppo Teal ha stimato nel 2013 che gli investimenti raddoppieranno nei prossimi dieci anni, passando dagli odierni 5,2 miliardi di dollari spesi nel settore ogni anno a 11,6 miliardi, per complessivi 89 miliardi nell'arco della decade.

Dall'uso prettamente militare dei droni a partire dai primi anni Duemila[1] si è man mano venuto estendendo anche il loro impiego in ambito civile. Tra le varie applicazioni della tecnologia, è il caso dell'uso dei droni per lo spegnimento degli incendi, il monitoraggio dell'ambiente, la spedizione e consegna di medicinali e altro ancora. Mentre all'inizio del 2014 sia *Amazon* sia *Facebook* hanno cominciato a pensare all'utilizzo dei droni ora per recapitare i propri pacchi ai clienti, ora per garantire una maggiore copertura globale per Internet, anche i legislatori nazionali non sono rimasti a guardare. Il 19 aprile 2016, a larghissima maggioranza, il Senato nordamericano ha approvato il disegno di legge 2658 – vale a dire il *Federal Aviation Administration (FAA) Reauthorization bill* – per accelerare l'impiego civile e commerciale di questa tecnologia. Poco prima, a marzo di quell'anno, l'ottava commissione del Senato italiano approvava, sia pure con riserva, la proposta di Regolamento del Parlamento europeo e del Consiglio sulle regole comuni nel settore dell'aviazione civile che, ai sensi del secondo protocollo del Trattato di Lisbona, richiede di essere sottoposto al vaglio preventivo degli Stati membri.

* Lara Merla è dottore in Giurisprudenza e praticante avvocato del Foro di Torino.

[1] Si veda P. SINGER, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, London, Penguin, 2009.

© Edizioni Scientifiche Italiane ISSN 0390-0975

Il suddetto Regolamento, in definitiva, mira ad abrogare il Regolamento CE n. 216/2008 che affida agli Stati membri la regolamentazione dei droni al di sotto dei 150 kg. In questo modo, verrebbe anche meno la disciplina adottata dall'Ente italiano per l'aviazione civile (ENAC), sulla quale avremo modo di tornare nel corso di queste pagine[2].

La prima corsa all'acquisto dei droni da parte dei comuni cittadini può farsi risalire al febbraio 2012, negli USA, ciò che ha comportato l'insorgere dei primi problemi nell'ambito di cui ci occupiamo in questo articolo, ossia il settore della privacy e della tutela dei dati personali. Emblematico il caso di un ragazzo di Seattle che, acquistato un drone, ha pensato bene di impiegarlo per spiare la propria ex-fidanzata[3]. Del 2015 è poi la notizia del quotidiano *Il Tempo*: "Frosinone: Scopre il tradimento della moglie con un drone". Il problema che gli studiosi hanno cominciato a porsi è dunque più che mai evidente: come disciplinare questi nuovi usi civili della robotica sulla base delle leggi attualmente vigenti nel campo della privacy e della protezione dei dati? Quali le differenze normative tra le due sponde dell'Oceano? E quali le diversità in Europa? Queste ultime saranno del tutto superate con l'entrata in vigore del nuovo Regolamento sulla protezione dei dati personali il 25 maggio 2018?

Al fine di dare una risposta il più possibile chiara ed esauriente a questi quesiti, la presente disamina viene suddivisa in quattro parti. Nel paragrafo successivo si preciserà il livello d'astrazione dal quale intendiamo far procedere la nostra analisi, vale a dire il punto di vista che assume il diritto come una meta-tecnologia. Su queste basi, il terzo paragrafo si occupa delle differenze esistenti tra Stati Uniti ed Europa, e cioè tra l'approccio settoriale tipico del modello statunitense nell'ambito della privacy e della protezione dei dati, e la vocazione generale del modello europeo, ribadita dal Regolamento Ue 2016/679 cui si è fatto cenno in precedenza[4]. Il quarto paragrafo mira a chiarire alcune specificità della disciplina italiana con particolare riguardo alla giurisprudenza della Corte di Cassazione in tema di videoriprese delle cosiddette immagini non comunicative. Seguiranno poi le conclusioni.

[2] Il riferimento va all'ultimo dei tormentati regolamenti messi a punto dall'ENAC sui "mezzi aerei a pilotaggio remoto" del 21 dicembre 2015, cui ha fatto seguito la Disposizione 29/DG del 1° aprile 2016 per la dilazione dei termini.

[3] Cfr. U. PAGALLO, *Il diritto nell'età dell'informazione*, Torino, Giappichelli, 2014, pp. 299-300.

[4] Si veda sin d'ora F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016.

ISSN 0390-0975 © Edizioni Scientifiche Italiane

2. Livelli d'astrazione

Con il termine "livello di astrazione" si precisa il piano dell'indagine dal quale conviene condurre il nostro discorso. Con il metodo proposto anni or sono da Luciano Floridi[5], l'idea è di mettere a punto l'interfaccia dell'analisi, grazie alla quale illustrarne "osservabili" e "variabili". Occorre spiegare sia i diversi modi in cui il legislatore può astrattamente pensare di regolare l'innovazione tecnologica sia come queste diverse modalità normative abbiano a che fare con un settore, quello della privacy e della protezione dei dati personali, continuamente messo alla prova dall'evolversi ed espandersi della tecnologia qui sotto esame, i "droni".

Nel caso delle modalità normative, un punto di riferimento è dato dalla definizione di diritto offerta da Hans Kelsen. Il teorico della *Grundnorm* proponeva il diritto come una tecnica di controllo sociale che si attua mediante la minaccia di misure coercitive: se A, allora B[6]. Una volta chiarito che oggetto di questa tecnica è la ricerca e sviluppo tecnologico, ne consegue che il diritto non solo possa essere inteso (anche) come una tecnica, ma soprattutto come una tecnica che regola un'altra tecnica, ossia una meta-tecnologia. Questo è il primo livello d'astrazione della nostra indagine, che sarà innanzitutto approfondito (par. 2.1). A seguire vedremo il modo in cui a sua volta la tecnologia incide sulle modalità tecniche con cui il diritto, appunto, mira a regolarla (par. 2.2).

2.1. Il diritto come meta-tecnologia

Ci sono due modi differenti in cui possiamo interpretare la formula kelseniana "se A, allora B". In un caso, l'attenzione viene posta su ciò che si suppone il diritto sia (condizioni); nell'altro, su quello che il diritto è chiamato a fare (funzioni). In quest'ultimo caso, si pensi alle diverse finalità che il legislatore può avere, e per le quali stabilisce le condizioni per cui, a una data fattispecie ("A"), seguiranno le sanzioni ("B"). Bert-Jaap Koops, ad esempio, ha proposto quattro diversi obiettivi che il legislatore può avere, nell'intento di regolare l'uso della tecnica. Si può mirare a raggiungere particolari effetti come la sicurezza nel trattamento e uso dei dati. In secondo luogo, il legislatore potrà stabilire, o meno, l'equivalenza funzionale tra attività online e

[5] L. Floridi, *The Method of Levels of Abstraction*, in "Minds and Machines", vol. 18, 2008, n. 3, pp. 303-329.

[6] H. Kelsen, *Dottrina pura del diritto*, 1934, I ed. (trad. it. Torino, Einaudi, 1952).

© Edizioni Scientifiche Italiane ISSN 0390-0975

offline: si rifletta sulla diversa disciplina normativa nel campo del copyright o tra un libro tradizionale e un e-book dato in licenza. In terzo luogo, la questione può ruotare attorno al principio di non discriminazione tra tecnologie con effetti equivalenti: si pensi, per fare un esempio, al caso della firma elettronica. Infine, in quarto luogo, Koops insiste sul fatto che, almeno in linea di principio, la legge non dovrebbe arrestare il progresso tecnologico, oppure richiedere di essere rivista e quindi aggiornata continuamente per via di questo stesso progresso[7].

Altri studiosi, come Chris Reed, suggeriscono di cogliere la natura meta-tecnologica del diritto secondo una tripartizione[8]. In particolare, occorrerebbe in primo luogo vagliare l'indifferenza tecnologica della legge, ossia se e in che misura le finalità perseguite dall'ordinamento valgano indipendentemente dalla tecnologia in gioco. È il caso dell'autorizzazione a comunicare le proprie opere al pubblico nell'ambito del diritto d'autore, per cui si tratta di un diritto d'esclusiva che vale a prescindere dalla dimensione, online/offline, e dalle modalità tecniche – quali streaming, DVD, p2p, ecc. – in cui dati e informazioni protetti dal diritto d'autore circolano. In secondo luogo, il richiamo va alla neutralità dell'implementazione e, cioè, al fatto che, una volta fissata la finalità da perseguire per legge – come nel ricordato caso delle firme elettroniche –, l'oggetto della disciplina non è specifico per una data tecnologia, ma, anzi, è indifferente alle sue possibili implementazioni. In terzo luogo, l'attenzione va a ciò che Reeds chiama la "potenziale neutralità della legge": quest'ultima specifica i requisiti di legittimità delle applicazioni tecnologiche, ma poi, come nel caso delle firme biometriche, consente che queste ultime modalità tecniche per la sottoscrizione di dati possano essere adeguate alle condizioni di legittimità disposte dall'ordinamento.

In un recente scritto Ronald Leenes e Federica Lucivero suggeriscono poi di cogliere l'intento regolativo del diritto nell'ambito della robotica, secondo una quadripartizione[9]. In primo luogo, si pensi alla disciplina dei progettisti e costruttori di robot, quali i droni, attuata attraverso la legge, come nel caso degli standard di sicurezza ISO o le norme sulla responsabilità civile e penale

[7] Si veda B-J KOOPS, *Should ICT Regulation Be Technology-neutral?*, in B-J Koops et al. (eds.), "Starting Points for ICT Regulation: Decostructing Prevalent Policy One-liners", pp. 77-108, The Hague, TMC Asser, 2006.

[8] Si veda C. REED, *Making Laws for Cyberspace*, Oxford, Oxford University Press, 2012.

[9] Cfr. R. LEENES, F. LUCIVERO, *Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design*, in "Law, Innovation and Technology", vol. 6, 2014, n. 2, pp. 193-220.

ISSN 0390-0975 © Edizioni Scientifiche Italiane

per produttori e utenti dei medesimi. In secondo luogo, il richiamo va alla regolazione del comportamento degli utenti e/o operatori dei droni, tramite il *design* di questi ultimi, vale a dire progettando queste macchine in modo tale che non sia consentito alcun comportamento illecito degli esseri umani. In terzo luogo, si può pensare alla disciplina legale degli effetti dei comportamenti robotici per il tramite delle leggi approntate dal legislatore: è il caso ad esempio della contrattualistica e negoziazione a mezzo di agenti software. In quarto luogo, infine, la legge può mirare alla disciplina del comportamento robotico tramite il suo *design*, ossia immettendo direttamente i dettami della legge nel software dell'agente robotico. In questo caso, ai metodi tradizionali di regolamentazione giuridica, sul piano del dover essere kelseniano "se A, allora B", si affianca – o viene sostituito da – l'intento regolativo della legge tramite il *design* dei ricavati tecnologici: nel nostro caso, i droni. Si tratta di una forma di tecno-regolazione giuridica sul piano dell'essere – o degli automatismi normativi – che approfondiamo a continuazione, all'insegna del cosiddetto principio della *privacy by design*.

2.2. *Il* design *della privacy*

L'intento regolativo che la legge persegue tramite il *design* dei droni rimanda in fondo a un approccio che possiamo far risalire alla prima disciplina europea in materia di trattamento e tutela dei dati personali: da un lato, fin dal considerando 46 della Direttiva 95/46/CE, si è richiesta «l'adozione di adeguate misure tecniche ed organizzative sia al momento della progettazione che a quello dell'esecuzione del trattamento». D'altro canto, la responsabilità per le misure tecniche appropriate è stata sancita fin dall'articolo 17(1) della stessa Direttiva, che afferma che «gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita», ecc.

Coniata alla fine degli anni Novanta dal Commissario per la privacy dell'Ontario, in Canada, Ann Cavoukian, la formula *privacy by design* sarebbe stata ripresa poco più tardi in alcuni testi ufficiali, tra cui il *Privacy Design Principles for an Integrated Justice System* presentato, nell'aprile 2000, dal Dipartimento della giustizia nordamericano e dal Commissario per la privacy dell'Ontario[10]. Successivamente, in Europa, il 1° dicembre 2009, il Gruppo

[10] Si veda A. CAVOUKIAN, *Privacy by Design: The Definitive Workshop*, in "Identity in the Information Society", vol. 3, 2010, n. 2, pp. 247-251.

© Edizioni Scientifiche Italiane ISSN 0390-0975

di lavoro ex art. 29, insieme al Gruppo di lavoro per la polizia e la giustizia, ha pubblicato un documento su "Il Futuro della Privacy", in cui viene dato ampio spazio, appunto, al «nuovo principio della *privacy by design*» che, a sua volta, torna nel nuovo Regolamento proposto dalla Commissione europea in materia di protezione dati, nel gennaio 2012, finalmente destinato a entrare in vigore, come detto, nel maggio 2018.

Anche di recente, la formula è stata significativamente ripresa dalle linee guida di uno studio finanziato dalla Commissione europea, "Robolaw", secondo cui, in sostanza, «l'emergente settore della *privacy by design* può servire a rendere e mantenere il comportamento dei robot nei limiti delle leggi in materia di protezione dati»[11]. Ma come fare in modo che ciò accada nel settore dei droni? Come declinare, in questo caso, le finalità regolative del tecno-diritto?

In questo caso, alcune disposizioni in tema di sicurezza dei dati, per fare un esempio, possono implementarsi nel software e nell'interfaccia della macchina robotica tramite dispositivi di criptazione e sistemi di controllo per l'accesso ai dati. Del pari, riprendendo le linee guida di Robolaw, alcuni «requisiti come il consenso informato possono essere implementati nella progettazione del sistema, ad esempio tramite l'interazione con gli utenti mediante schermi e dispositivi di caricamento [input]»[12]. In fondo, questo è ciò che accade già con alcuni sistemi operativi in commercio, come nel caso di Android, che richiedono il consenso dell'utente ogni qualvolta un'applicazione intenda fare uso dei loro dati personali. Inoltre, possiamo anche pensare ai droni configurati in modo tale che l'insieme dei dati da raccogliere e processare sia ridotto al minimo, in omaggio al principio della finalità del trattamento. Ai sensi dell'articolo 6(1)(b) della ricordata Direttiva 46 del 1995, questo significa che i droni dovrebbero raccogliere dati soltanto nella misura in cui ciò sia necessario per espletare un compito specifico e legittimo. Per cui, da un lato, sempre secondo le linee guida di Robolaw, «come corollario della valutazione d'impatto, dovrebbe implementarsi un meccanismo di controllo che accerti quando le tecnologie sono costruite nel modo più consono per la tutela della privacy e compatibilmente con altre istanze (quali bisogni d'informazione e sicurezza)»[13]. D'altro canto, «l'adozione di misure di sicurezza aggiornate non dovrebbe essere considerata una sempli-

[11] ROBOLAW, *Guidelines on Regulating Robotics. EU Project on Regulating Emerging Robotic Technologies in Europe: Robotics Facing Law and Ethics*, 2014, p. 19.

[12] *Ibidem*.

[13] *Ivi*, p. 190.

ISSN 0390-0975 © Edizioni Scientifiche Italiane

ce scelta dell'utente, bensì uno specifico obbligo giuridico. Appare chiaro che è improbabile che il trattamento illecito dei dati sia considerato una responsabilità dei costruttori di robot, ma piuttosto dell'utente, che può essere ritenuto "custode" dei dati personali»[14].

Naturalmente, tuttavia, il diavolo, come suol dirsi, è nei dettagli. L'applicazione dei concetti giuridici dipende infatti, molto spesso, dal contesto in cui tali concetti devono essere interpretati[15]. Un esempio è dato proprio dal settore della protezione dei dati personali, in cui già solo quest'ultima nozione, al pari di altre – come "misure di sicurezza" o "controllore dei dati" –, non può essere del tutto de-contestualizzata e, quindi, sorge il sospetto che ciò che può diventare arduo decodificare a un umano esperto nel settore giuridico a maggior ragione diventi un'impresa impossibile da compiere per un drone[16].

In aggiunta, sembra discutibile la tesi di Robolaw che sia sempre e solo l'utente del drone ad essere il "custode" dei dati personali e, per ciò stesso, responsabile per ogni possibile uso o trattamento illecito. Basterebbe pensare a quanto accade già al giorno d'oggi circa le questioni relative alla connettività su Internet, con le applicazioni per i servizi mobili, come i nostri *smartphone*, oppure con i sensori. Ci sono molte circostanze in cui il trattamento illecito dei dati personali ben può dipendere dal modo in cui il drone è stato disegnato o costruito, dalla negligenza del fornitore di connettività o di coloro i quali sviluppano determinati applicativi. Il trattamento illecito dei dati personali potrebbe così farsi risalire al mal funzionamento del drone, all'intestazione dei pacchetti di traffico in rete (http) che possono essere impiegati per determinare gli interessi o altra informazione personale relativa all'utente o a terzi, di pari passo con applicazioni che lascino trapelare dati identificativi delle persone, attraverso, ad esempio, GPS o altro ancora.

Come se non bastasse, rimangono poi aperti i problemi relativi, ora, alle differenze, anche sostanziali, che si danno tra i diversi sistemi normativi, come nel caso degli Stati Uniti d'America e dell'Europa, ora riguardo al modo di interpretare alcune nozioni chiave di questi stessi sistemi, come nel caso, su cui ritorneremo, del principio della *privacy by design* nell'ordina-

[14] *Ibidem*.

[15] Si veda, ad esempio, il Parere 1/2010 del Gruppo di lavoro art. 29, per cui «il concetto di controllore [dei dati] è funzionale, inteso a stabilire la responsabilità [per il trattamento dei dati], dove si trova l'influenza di fatto e per ciò fondato su un'analisi fattuale, piuttosto che formale» (WP 169, p. 9).

[16] Cfr. ancora il Gruppo di lavoro art. 29 sui "Recenti sviluppi dell'Internet delle cose" (Parere 8/2014, WP 223).

© Edizioni Scientifiche Italiane ISSN 0390-0975

mento dell'Ue. Prima di tornare alle varie opzioni aperte al diritto come meta-tecnologia e ai possibili impieghi della tecno-regolazione giuridica nel campo dei droni, bisogna passare brevemente in rassegna le basilari differenze in tema di privacy e tutela dei dati personali tra USA e Ue, e all'interno di quest'ultima, tra gli Stati membri.

3. Tra Stati Uniti e Unione europea

Notoriamente, le due aree di cui trattiamo in questo articolo, e cioè gli Stati Uniti d'America e l'Europa, hanno una visione degli istituti qui in esame per molti versi dissimile. Ciò sia per quanto concerne il grado di protezione che viene comunemente accordato ai cittadini in ragione delle esigenze della sicurezza nazionale o del diritto all'informazione, sia per quanto riguarda il modo in cui il legislatore, da un parte, e i giudici, dall'altra, elaborano e applicano il diritto. Nell'Unione europea, occorre partire dalla distinzione tra la tutela della privacy e la protezione dei dati personali. Secondo la Carta dei diritti fondamentali dell'Unione europea, bisogna infatti distinguere dalla tutela dell'art. 7, per cui «ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni», l'art. 8, che si occupa della protezione dei dati di carattere personale. Al diritto in generale, si affiancano poi il diritto a che i dati siano trattati in modo leale, il diritto d'accesso e di rettifica, laddove il rispetto di tali regole è soggetto al controllo di un'autorità indipendente. Fondato su queste basi costituzionali, si può pertanto dire che il modello europeo della privacy e della tutela dei dati personali si presenta come un sistema a vocazione "generale" con alcuni tratti tipici degli assetti giuridici federali. Al piano costituzionale delle fonti, definito dai Trattati, bisogna aggiungere i principi che la Corte di Giustizia ha ricavato dalle tradizioni giuridiche comuni degli Stati membri e, a vario titolo, dai diritti proclamati dalle convenzioni e dichiarazioni internazionali. Sul piano della legislazione secondaria, questa serie di principi è stata implementata da vent'anni a questa parte con una prima generazione di direttive, quali la Direttiva 95/46/CE e la Direttiva 2002/58/CE sul trattamento dei dati personali e la tutela della vita privata nelle comunicazioni elettroniche, fino all'accennato nuovo Regolamento Ue 2016/679.

Il modello americano della privacy può a sua volta essere descritto come un sistema a "vocazione settoriale"[17]. Sebbene esista un quadro normativo

[17] Si veda U. Pagallo, *La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, Milano, Giuffrè, 2008.

ISSN 0390-0975 © Edizioni Scientifiche Italiane

generale, sostanzialmente riconducibile alle decisioni della Corte Suprema di Washington, la tutela della privacy e dei dati personali negli USA è affidata a una serie nutrita di leggi o statuti, sul piano sia federale sia statale. Per riprendere le tesi di Pagallo[18], la natura "settoriale" del modello americano è dipesa dalla necessità di rispondere tempestivamente sia agli scandali occorsi, più spesso, a partire dai primi anni Settanta del Novecento sia ai vuoti normativi prodotti dal progresso e dall'evoluzione tecnologica. Sul primo fronte va ricordato il *Privacy Act* del 1974 con il quale il Congresso di Washington rispose allo scandalo del Watergate con le dimissioni del presidente Richard Nixon; oppure, il *Video Privacy Protection Act* del 1988, approvato dal Congresso poco dopo ciò che era capitato al giudice Robert Bork, del quale, durante le audizioni per la sua conferma a membro della Corte Suprema, la stampa finì per pubblicare la lista delle videocassette prese a noleggio. Per quanto riguarda l'evoluzione tecnologica, basti segnalare il *Cable Communications Policy Act* del 1984, l'*Electronic Communications Privacy Act* del 1986, lo *Health Insurance Portability and Accountability Act* del 1996, l'*Identity Theft and Assumption Deterrence Act* del 1998, il *CAN-SPAM Act* del 2003, fino al *Video Voyeurism Prevention Act* del 2004.

Mettendo a confronto Stati Uniti ed Europa, il risultato del diverso quadro normativo è che, negli USA, il problema per l'uso dei droni nel campo della privacy e della tutela dei dati personali non è esaminato secondo i principi e le norme di una disciplina unitaria, come nel caso del ricordato Regolamento Ue 2016/679. Piuttosto, il riferimento va alla vigente disciplina in tema di intercettazioni, video-voyeurismo, leggi sui paparazzi e diritto di cronaca che, su scala prevalentemente statale, più che federale, regolano l'uso di fotografie, video o audio, potenzialmente intrusivi per la privacy[19]. Inoltre, l'uso dei droni ripropone la tormentata storia, tutta americana, sulla ragionevole aspettativa di tutela nei luoghi pubblici. Nonostante alcune importanti decisioni della Corte Suprema di Washington, a far data dal caso Katz del 1967, non soltanto molte Corti statunitensi si sono mostrate riluttanti a riconoscere una ragionevole aspettativa di privacy nei luoghi pubblici, come avviene nel caso dei droni[20]; ma, si è ammessa anche la peculiarità dei problemi giuridici posti dal loro uso. In fondo, si assommano in un'applicazione

[18] *Ibidem*.

[19] Cfr. M.E. KAMINSKI, *Drone Federalism: Civilian Drones and the Things They Carry*, in "California Law Review Circuit", 2013, n. 4, pp. 57-74.

[20] Si veda N. DANFORTH ZERONDA, *Street Shootings: Covert Photography and Public Privacy*, in "Vanderbilt Law Review", 2010, n. 63, pp. 1131-1159.

© Edizioni Scientifiche Italiane ISSN 0390-0975

unica i problemi sollevati dalle tecniche dell'intercettazione, rintracciabilità delle persone e dei luoghi, video sorveglianza, cattura delle immagini e così via. Il risultato è che, negli Stati Uniti, sono stati già presentati diversi disegni di legge, a livello sia statale sia federale, al fine di vietare le fotografie e le video-riprese fatte dai droni senza il consenso degli interessati, e di limitare l'uso di immagini e altre informazioni da parte dei civili. Basti far cenno al *Texas Privacy Act* (H.B. 912 del 2013), al *Preserving American Privacy Act* (H.R. 637 del 2013), ecc.

In Europa, la vocazione generale del modello suggerisce di prestare attenzione al quadro di diritti, garanzie e obblighi destinati a uscire rafforzati con il Regolamento 2016/679. Come il sito della Commissione è lieto di informarci, «l'obiettivo di questo nuovo insieme di regole è di ridare controllo ai cittadini sui propri dati personali, e di semplificare il quadro regolativo per l'attività economica (business). La riforma della protezione dati è uno snodo cruciale per il singolo mercato digitale che la Commissione annovera fra le sue priorità. La riforma consentirà ai cittadini europei e agli imprenditori di beneficiare pienamente dell'economia digitale».

Eppure, anche in Europa e in previsione dell'entrata in regime del Regolamento, l'uso dei droni è destinato a sollevare una serie complessa di problemi. Alcuni concernono la sicurezza dei voli che la proposta del Parlamento europeo e del Consiglio ha inteso affrontare con il nuovo Regolamento ricordato nell'introduzione. Dal punto di vista del diritto come meta-tecnologia, bisogna fissare le regole comuni nel settore dell'aviazione civile che permettano il volo degli RPAs. Altri dilemmi investono la ripartizione di competenze tra Stati membri (SM) e Ue proprio nel settore della privacy e della tutela dei dati personali. I limiti che in nome della sicurezza nazionale e dell'ordine pubblico di ogni SM erano stati fissati alle competenze dell'Ue con gli articoli 3 e 13 della prima Direttiva 95/46/CE, ritornano del pari nel nuovo Regolamento. Anche se, con riguardo al quadro normativo che ci attende nei prossimi anni, il riferimento va non solo al nuovo Regolamento che diverrà a tutti gli effetti legge dal 25 maggio 2018, ma anche alla nuova Direttiva che entrerà in vigore il 6 maggio di quello stesso anno, sulla «protezione delle persone fisiche in rapporto al trattamento di dati personali da parte di autorità preposte al fine di prevenire, investigare, intercettare o perseguire delitti o applicare sanzioni penali». In sostanza, si vuole suggerire che il nuovo Regolamento lascia sin d'ora aperti alcuni dei problemi chiave della nostra indagine, come nel caso del *design* dei droni cui si è fatto riferimento nel paragrafo precedente. Inoltre, dal punto di vista del diritto come meta-tecnologia è interessante

ISSN 0390-0975 © Edizioni Scientifiche Italiane

notare come la ripartizione delle competenze tra SM e Ue nel nuovo Regolamento avvalla alcune disparità di trattamento che si sono già verificate (e denunciate) in questi ultimi anni. Si pensi ad esempio al caso in cui, in Italia, un soggetto decida di spiare un privato con l'utilizzo di un drone. Mentre un giurista in America dovrebbe vagliare le varie leggi sulle intercettazioni, il video-voyeurismo, le norme sui paparazzi, il diritto di parola o di cronaca, fino alla fondamentale sentenza della Corte Suprema nel caso Jones[21], a quali norme e principi deve fare soprattutto attenzione un giurista in Italia?

4. Tra Unione europea e Italia

Si è già detto che il modello europeo della privacy si presenta come un sistema a vocazione "generale", con alcuni tratti tipici degli assetti giuridici federali. Al piano costituzionale delle fonti, definito dai Trattati e dalla giurisprudenza della Corte di Giustizia, si aggiunge la fitta serie di disposizioni secondarie. Nel nostro caso si tratta della prima generazione di direttive in materia di trattamento e tutela dei dati personali, cui si accompagna un "controllo diffuso" di costituzionalità delle leggi operato dalla stessa Corte europea, nel rapporto con i giudici nazionali tenuti a non-applicare la normativa degli Stati membri in caso di contrasto. Risolvendo le controversie su base comunitaria, e con la possibilità di ricorrere in via pregiudiziale alla Corte di Giustizia quale organo preposto a chiusura del sistema, si ha pertanto un'armonizzazione dei diritti nazionali che punta a una tutela piena nel trattamento dei dati delle persone in (quasi) tutto il continente.

D'altra parte, si è riferito dei limiti strutturali che segnano il modello europeo con l'esempio che qualcuno, come occorso qualche tempo fa a Frosinone, spii in Italia un privato con l'utilizzo dei droni. *Quid iuris*? Oltre alla normativa del codice della privacy, il caso ricadrebbe infatti sotto l'art. 615 *bis* del nostro codice penale, che configura il reato di interferenze illecite nella vita delle persone. Il raccordo tra il codice della privacy e il codice penale però si complica, avendo a mente un duplice ordine di fattori costituzionali che entrano qui in gioco. In primo luogo, si tenga presente ciò che, secondo il gergo giuridico italiano, si definisce come "videoriprese di immagini non comunicative", che possono essere disposte anche senza l'intervento di un

[21] Il richiamo va a *United States vs. Jones* (565 U.S.), con cui, il 23 febbraio 2012, la Corte Suprema americana ha dichiarato illegittima la sorveglianza continua tramite GPS, priva dell'autorizzazione di un giudice. Sul caso si veda U. Pagallo, *Il diritto nell'età dell'informazione*, cit., pp. 211-217.

© Edizioni Scientifiche Italiane ISSN 0390-0975

soggetto terzo e indipendente, quale il giudice. In secondo luogo, per ciò che riguarda la tutela del domicilio, l'interpretazione che di esso ne danno le Corti è restrittiva. Non bisogna intendere la nozione di domicilio di cui all'art. 14 Cost. nel suo significato oggettivo, mutuato dal codice civile e ripreso dall'art. 614 del codice penale. Piuttosto, affinché scatti la tutela alla propria riservatezza, come dichiarato dalla Corte Costituzionale nel 2008, occorre che l'individuo abbia un rapporto stabile con quel luogo e, soprattutto, che i suoi comportamenti nella dimora privata non siano visibili a terzi. Come si esprime la Corte: «affinché scatti la protezione dell'art. 14 Cost., non basta che un certo comportamento venga tenuto in luoghi di privata dimora; ma occorre, altresì, che esso avvenga in condizioni tali da renderlo tendenzialmente non visibile a terzi» (sentenza n. 149 del 7 maggio 2008). Su tali basi è intervenuta in seguito anche la Cassazione in senso ancor più restrittivo, distinguendo la tutela costituzionale del domicilio dal diritto alla riservatezza fondato sull'art. 2 Cost., per cui la dignità delle persone godrebbe di un grado di tutela inferiore di quello accordato alla tutela del domicilio, delle comunicazioni e della libertà personale. «La tutela costituzionale del domicilio – afferma infatti la Corte – va limitata ai luoghi con i quali la persona abbia un rapporto stabile, sicché, quando si tratti di tutelare solo la riservatezza, la prova atipica, quale è una videoregistrazione, può essere ammessa con provvedimento motivato dell'autorità giudiziaria. Non sono quindi ammissibili riprese visive effettuate, ai fini del processo, in ambito domiciliare, mentre vanno autorizzate dall'autorità giudiziaria procedente, cioè p.m. o giudice, le riprese visive che, pur non comportando un'intrusione domiciliare, violino la riservatezza personale»[22].

Appare qui doveroso sottolineare lo sconcerto che tali orientamenti hanno suscitato in dottrina, dato che il diritto alla riservatezza viene ricondotto alla sfera di tutela dell'art. 2 Cost., in tema di dignità personale, e non all'art. 14, in base a cui si avrebbe invece la doppia riserva di legge e di giurisdizione accordata alla protezione della "inviolabilità" del proprio domicilio[23]. Paradossalmente, si potrebbe anche sostenere che alla mancanza di garanzie approntate dalla Consulta e dalla Suprema Corte, abbia sopperito l'ENAC con la ricordata fitta serie di disposizioni volte a garantire la sicurezza del traffi-

[22] Cass., sez. VI penale, sentenza 33953 del 15 giugno 2012.

[23] Si veda M. SENOR, *Videoriprese di immagini non comunicative: un vuoto legislativo che la giurisprudenza non intende colmare con un'interpretazione garantista*, in "Penale.it", 2012, http://www.penale.it/stampa.asp?idpag=1079. Cfr. inoltre M. ALOVISIO, D. BURRONI, A. FROSINI, E.O. POLICELLA (a cura di), *Videosorveglianza e privacy*, Forlì, Experta, 2011.

ISSN 0390-0975 © Edizioni Scientifiche Italiane

co aereo. Come accennato, i regolamenti che si sono venuti accumulando tra il 2013 e il 2016, sono tali da rendere, allo stato attuale, spesso impraticabile l'impiego legittimo di droni per usi civili in Italia! In sostanza, non dovremmo preoccuparci della mancanza di tutela per il possibile impatto dei droni sulla nostra vita privata, perché, semplicemente, allo stato "il fatto non sussiste"[24].

Tuttavia, ci sono due ragioni per le quali occorre procedere oltre con l'analisi. In primo luogo, l'uso civile dei droni va affermandosi in altri Stati membri dell'Unione europea, come la Germania: si tratta del servizio di recapito di medicinali in alcune isole del Mare del Nord a cura della DHL[25]. In secondo luogo, c'è da aspettarsi che perfino in Italia, e con buona pace dell'ENAC, sia soltanto una questione di tempo per avere una disciplina più ragionevole dell'intero settore, ossia il ricordato Regolamento per l'aviazione civile e, più in particolare, per i droni sotto i 150 kg. Appare opportuno che l'uso legittimo di tali dispositivi per la protezione civile, l'agricoltura, il commercio o perfino le arti, non venga impedito da parte dell'autorità che detta le regole di settore. Il risultato è però che torna a proporsi in questo modo il problema di come regolare il possibile impatto di queste applicazioni robotiche sulla privacy e sul regime della protezione dei dati personali.

Alla luce del quadro generale della normativa messo a punto nelle parti precedenti dell'analisi, si tratta ora di riassumere quali nuove sfide dobbiamo attenderci ragionevolmente nel futuro.

5. Conclusioni

Il presente articolo su privacy, dati personali e droni è partito dal livello d'astrazione del diritto come meta-tecnologia, per cogliere i diversi modi in cui i legislatori, nazionali e internazionali, hanno inteso disciplinare la materia (par. 2), per ciò stesso mostrando alcune differenze significative tra USA e Ue (par. 3), e all'interno di quest'ultima tra Stati membri (par. 4).

In primo luogo, tornando alle tesi di Bert-Jaap Koops sui quattro diversi obiettivi che il legislatore può avere nell'intento di regolare l'uso della tec-

[24] Si vedano il *Regolamento ENAC "Mezzi Aerei a Pilotaggio Remoto"* del 16 dicembre 2013, cui ha fatto seguito prima la modifica dell'articolo 26 con *Disposizione 4/DG* del 14 febbraio 2014, e poi la *Disposizione 8/DG* del 16 marzo 2015, https://www.enac.gov.it/La_Normativa/Normativa_Enac/Regolamenti/Regolamenti_ad_hoc/info-122671512.html.

[25] Cfr. http://www.livescience.com/48032-dhl-drone-delivery-service.html (con video annesso).

© Edizioni Scientifiche Italiane ISSN 0390-0975

nica, si può notare, tanto negli USA quanto nell'Ue, l'obiettivo di ottenere l'equivalenza funzionale tra aereo tradizionale e uso dei droni. La tecnica è quella di arrivare a raggiungere particolari effetti sia in modo tradizionale, secondo i dettami kelseniani del "se A, allora B", sia immettendo le regole giuridiche nella tecnologia stessa, secondo il principio della *privacy by design* e i dettami del tecno-diritto. In ogni caso, la legge non dovrebbe arrestare il progresso tecnologico, oppure richiedere di essere rivista e quindi aggiornata continuamente per via di questo stesso progresso, come invece è capitato con la sfilza di regolamenti accumulati negli ultimi anni dall'ENAC in materia. Sul piano del diritto come meta-tecnologia e per riprendere le tesi di Chris Reed, un buon metodo per raggiungere tale obiettivo è dato dal principio dell'indifferenza tecnologica della legge. Ciò significa che le diverse finalità perseguite dall'ordinamento in materia di privacy e tutela dei dati valgono indipendentemente dalla tecnologia in gioco e dalle diverse possibili implementazioni. Questo principio può essere attuato ora in modo tradizionale, ora con le modalità del tecno-diritto. Nel primo caso, si pensi ancora alla disciplina dei progettisti e costruttori di robot mediante la legge, come nel caso delle norme sulla responsabilità civile e penale per produttori e utenti di robot. Nel secondo caso, si può puntare a disciplinare ora il comportamento degli utenti e/o operatori dei droni, tramite il *design* di questi ultimi, ora lo stesso comportamento robotico, immettendo direttamente i dettami della legge nel software dell'agente artificiale. Questo duplice livello d'intervento del legislatore, sia sul piano sanzionatorio tradizionale attinente alla sfera del dover essere, sia sul piano del disegno tecnologico del drone, mette in risalto tanto le differenze giuridiche che permangono tra USA e Ue, e tra Stati membri di quest'ultima, quanto alcuni nodi aperti con le istanze della tecno-regolazione giuridica.

In secondo luogo, infatti, il presente articolo si è incaricato di sottolineare alcune differenze cardine di giurisdizione caratterizzanti il settore. Il par. 3 ha messo in luce la distanza tra la vocazione generale del modello europeo della privacy e della tutela dei dati personali, con l'approccio settoriale invalso negli Stati Uniti. Mentre, in quest'ultimo ordinamento, la questione ruota attorno a come aggiungere una nuova legge specifica che governi il settore, nell'Ue il problema è come applicare, negli anni a venire, le nuove disposizioni del Regolamento 2016/679. Come evidenziato dal par. 4, anche l'entrata in vigore di queste disposizioni non scioglierà tuttavia alcune disparità di trattamento e di tutela all'interno dell'Ue, secondo ciò che si è avuto modo di evidenziare con i richiami alla giurisprudenza della Corte italiana di Cassazione

ISSN 0390-0975 © Edizioni Scientifiche Italiane

in tema di video-riprese di immagini non comunicative. Quanto è consentito fare alle forze dell'ordine in Italia sarebbe illegittimo negli USA dopo la decisione della Corte Suprema nel caso Jones[26]. Il permanere di queste fondamentali differenze tra sistemi giuridici ripropone con forza i nodi aperti con la tecno-regolazione. Quale insieme di norme e principi, di tipo statunitense o europeo, dobbiamo prescegliere e poi immettere nel *design* dei droni?

In terzo luogo, è proprio il Regolamento Ue 2016/679 a suggerire come alcune delle questioni innescate, o proposte, dall'uso dei droni siano destinate a rimanere aperte anche dopo l'entrata in vigore del nuovo quadro normativo. Ritornando al principio della *privacy by design*, disciplinato dall'art. 25 del Regolamento, in raccordo con il meccanismo certificativo di cui al successivo art. 42 e con le regole vincolanti dell'art. 47(2)(d), il fine che questo uso della tecno-regolamentazione potrà mai avere appare poco chiaro. Per un verso, la tutela dei dati passa attraverso le misure digitali di sicurezza che mirano ad attenuare l'impatto dei comportamenti dannosi sulle persone o sui sistemi tecnologici dell'informazione e comunicazione. Basti pensare alla configurazione di base delle interfacce dei sistemi informatici, per cui il disegno dell'applicazione robotica può essere impostato in modo da essere appropriato all'uso anche da parte dei meno esperti e, tuttavia, senza che per questo il sistema smetta di aumentare la propria efficienza. Al pari di altre modalità per la sicurezza, come la configurazione dell'interfaccia dei sistemi informatici o delle copie di riserva o *backup*, l'obiettivo di questa modalità del *design* non è, dunque, quello di impedire che un evento dannoso si verifichi ma, piuttosto, nel caso in cui quest'ultimo si materializzi, che il sistema sia preparato a tutelarsi. Ecco perché si è suggerito un parallelismo tra questo tipo di *design* e gli *airbag* delle automobili:[27] l'idea non è né di invogliare gli automobilisti a cambiare direttamente stile di guida, né di impedire che si verifichino incidenti. Piuttosto, nel caso d'incidente, l'intento è appunto quello di attutirne, in tutto o in parte, gli effetti.

Questa regolazione della tecnologia può naturalmente essere disegnata in automatico e riportata alle finalità del diritto come meta-tecnologia, illustrate in questo articolo. L'intento tecno-regolativo del diritto ha infatti a che fare, in questo caso, più con l'affidabilità e meticolosità del disegno delle misure di sicurezza in questione che con le ricadute sull'autonomia dei soggetti. Si tratta di una differenza critica con l'altro intento tecno-regolativo del diritto

[26] Si veda *supra* nota 21.

[27] U. PAGALLO, *Il diritto nell'età dell'informazione*, cit., p. 139.

© Edizioni Scientifiche Italiane ISSN 0390-0975

che riguarda la finalità del *design* di prevenire del tutto che comportamenti dannosi si verifichino. Oltre agli esempi dell'impiego di DRM - *Digital Rights Management* nel campo della proprietà intellettuale, o dell'uso di sistemi di filtraggio in rete ai fini della sicurezza nazionale, questo può essere il caso della *privacy by design* nell'ambito della robotica e, in particolar modo, dei droni. Come riferito in precedenza, riprendendo le tesi di Leenes e Lucivero[28], l'obiettivo può riguardare sia la regolazione del comportamento degli utenti e/o operatori dei robot, tramite il *design* di questi ultimi, in modo tale cioè che non sia consentito alcun comportamento illecito degli esseri umani, sia la disciplina del comportamento robotico tramite il loro *design*, ossia immettendo direttamente i dettami della legge nel software dell'agente robotico, in modo tale da prevenirne atti indesiderati. Si tratta di un approccio al principio della *privacy by design* reso popolare proprio dalla sua stessa inventrice, il ricordato Commissario per la privacy dell'Ontario, Ann Cavoukian[29]. Superati i problemi tecnici di sicurezza sul volo dei droni, ci sarebbe anche il modo di prevenire del tutto la violazione della tutela dei dati personali nel loro intero ciclo di vita, per così dire dalla culla alla tomba.

Tuttavia, esiste una serie di ragioni ulteriori per cui l'obiettivo del *design* a controllo totale presenta una serie di problematiche. La prima è di natura tecnica e riporta, in parte, all'obiettiva difficoltà di formalizzare alcuni concetti cardine della disciplina in materia di privacy e protezione dati, spesso dipendenti dal contesto preso in esame e soggetti peraltro ad evoluzione. Come ricorda Karen Yeung, «non solo è inevitabile il rischio di fallimenti operativi, ma la finalità di disegnare standard che siano in grado di raggiungere l'obiettivo desiderato dal regolatore in forma precisa e accurata non può che essere, con ogni evenienza, un'impresa improba»[30].

Una seconda ragione di perplessità è poi suggerita da un'ampia e comprovata letteratura scientifica che evidenzia il modo in cui particolari configurazioni di valori sociali, etici o politici, siano direttamente e sistematicamente realizzati, o soppressi, dal disegno tecnologico[31]. Avendo a mente le differen-

[28] Cfr. R. LEENES, F. LUCIVERO, *op. cit.*

[29] Si veda ancora A. CAVOUKIAN, *op. cit.*

[30] K. YEUNG, *Towards an Understanding of Regulation by Design*, in R. Brownsword, K. Yeung (eds.), "Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes", London, Hart, 2007, p. 106.

[31] Cfr. M. FLANAGAN, D.C. HOWE, H. NISSENBAUM, *Embodying Values in Technology: Theory and Practice*, in J. van den Hoven, J. Weckert (eds.), "Information Technology and Moral Philosophy", New York, Cambridge University Press, 2008, pp. 322-353.

ISSN 0390-0975 © Edizioni Scientifiche Italiane

ze, anche radicali, appurate nel corso del presente articolo, a proposito delle diverse forme che il diritto alla privacy e la tutela dei dati personali assumono negli Stati Uniti e nell'Unione europea, c'è da sospettare che questa forma di *design* finisca per aggravare, piuttosto che risolvere, tali differenze. Basti pensare alla diatriba sulla configurazione dei sistemi a interfaccia informatica, tra il tradizionale approccio *opt-in* (*option-in*: consenso preventivo) europeo e il consueto modello di *opt-out* (*option-out*: disdetta successiva) invalso invece in America.

Infine, pesano ragioni di ordine giuridico. Da un lato, di fronte alla presunta infallibilità di una tecnologia automatizzata bisogna ricordare l'ammonimento di Lawrence Lessig, secondo cui «I controlli sull'accesso ai contenuti non saranno ratificati dai tribunali; saranno controlli inseriti dai programmatori tramite il codice. E, mentre i controlli introdotti per legge sono sempre verificati da un giudice, quelli inseriti nella tecnologia sono sprovvisti di analoghi riscontri»[32]. D'altro canto, per dirla con Jonathan Zittrain, «la perfetta applicabilità [della legge] fa svanire la pubblica comprensione del diritto in quanto la sua applicazione [automatica] elimina un'utile interfaccia tra i termini della legge e la sua imposizione. Parte di ciò che ci rende umani sono le scelte che facciamo ogni giorno su quel che rappresenta alcunché di giusto o sbagliato (...). In un ambiente monitorato e sorvegliato del tutto, quelle stesse scelte svaniscono»[33].

Bisognerà dunque attendere i prossimi anni per vedere quale delle due ottiche prevarrà tra il diritto come meta-tecnologia e il tecno-diritto (par. 2), tra USA e Ue (par. 3), e tra l'odierna giurisprudenza della Cassazione e una più consona interpretazione costituzionale del diritto alla privacy e alla tutela dei dati in Italia (par. 4). Sin d'ora è però facile prevedere che uno degli ambiti della ricerca contemporanea più ricco di finanziamenti come la robotica, vale a dire il settore dei droni, sia destinato a far crescere l'attenzione di politici e affaristi, giuristi ed economisti, semplici cittadini e imprese, per le ricadute nel campo della privacy e della tutela dei dati personali.

[32] L. LESSIG, *Free Culture: The Nature and Future of Creativity*, New York, Penguin Press, 2004, p. 152, trad. it. *Cultura libera*, Milano, Apogeo, 2005.

[33] J. ZITTRAIN, *Perfect Enforcement on Tomorrow's Internet*, in R. Brownsword, K. Yeung (eds.), "Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes", London, Hart, 2007, pp. 125-156 (come tradotto in M. DURANTE, U. PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, Utet, 2012, p. XX).

© Edizioni Scientifiche Italiane ISSN 0390-0975