La protezione dei dati personali al tempo degli algoritmi intelligenti e dei robot umanoidi

di **RICCARDO PISELLI**

Abstract

This paper addresses the mutual interrelations between the new right to privacy and the latest applications of Artificial Intelligence (AI) and robotics. On the one hand, being personal data the essential resource for the digital economy, AI and robots raises multiples privacy concerns in terms of direct surveillance and private spaces' intrusions. On the other, following the enactment of the General Data Protection Reform, the emergence of new privacy rights and the functional shift of the right to privacy are predicted to have disruptive consequences on the innovation in the field of AI and robotics. Rights such as the right to cancellation and the right to data portability question the economic nature of data as commodities. An unprecedented blending of disciplines emerge in that area with regard of machine learning and deep learning algorithms, which use data as the raw material of knowledge.

1. Premessa. «È il fatto di essere visto incessantemente, di poter sempre essere visto, che mantiene in soggezione l'individuo disciplinare» scrive Michel Foucault in *Sorvegliare e punire*: nella prigione perfetta il sorvegliato non sa mai esattamente quando è sorvegliato e la cosiddetta "veduta diseguale" lo conduce ad un'autodisciplina inesorabile, o a quello che Foucault chiama il "corpo docile". E' la stessa teoria al cuore del *panoptismo* ideato da Jeremy Bentham. Ma siamo davvero sicuri che questi meccanismi valgano solo nella particolarità della detenzione?

Non è forse attraverso questi stessi parametri che dobbiamo cominciare oggi a misurare anche la nostra libertà, includendo la coscienza di ciò che di noi è perennemente controllato da altri anche a nostra insaputa?

La strepitosa estensione della tecnologia a disposizione del Grande Fratello impone un veloce e radicale ribaltamento di tutte le prospettive.

Ecco allora che Intelligenza artificiale e diritto alla privacy appaiono improvvisamente tra loro legati sotto diversi profili.

Da un lato, le più recenti applicazioni della Intelligenza artificiale, facilitando l'acquisizione d'informazioni personali, moltiplicano le potenziali intrusioni nella sfera di riservatezza di ciascuno. Tale dialettica conflittuale, invero, non è nuova ed ha caratterizzato anche i rapporti tra più classiche tecnologie dell'informazione e diritto alla riservatezza (CHEMERINSKY 2007; GAVISON 1980).

Dall'altro lato, specularmente, la moderna evoluzione del diritto alla *privacy* introduce nuovi limiti allo sviluppo e alla diffusione dell'Intelligenza artificiale.

Il presente lavoro intende esplorare tale tensione alla luce delle ultime innovazioni tecnologiche e dell'imminente recepimento della General Data Protection Reform.

2. L'intelligenza artificiale. Algoritmo, informazione e memoria. Nella storia delle civiltà nulla sembra avere maggiormente affascinato l'uomo quanto l'evoluzione della conoscenza, lo studio dei meccanismi della mente: dalla maieutica socratica ai sistemi aristotelici, dall'episteme neoplatonica al dualismo cartesiano, dalla sostanza di Spinoza all'innatismo di Leibniz fino alla sintesi di Kant fra ragion pura e ragion pratica, dal sistema logico-ontoloigico di Hegel fino alle moderne teorie cognitive.

La storia dell'Intelligenza Artificiale (da ora I.A.) può essere scandita in tre fasi. La prima vede lo sviluppo di sistemi intelligenti nell'ambito della computazione. La seconda è caratterizzata dall'imitazione dei processi di soluzione di problemi e dei ragionamenti umani. La terza, infine, si

contraddistingue per la creazione di sistemi "esperti" e modelli cc.dd. "connessionisti (WARWICK 2012).

Più recentemente, con la progressiva attenzione prestata da legislatori e *policymakers* al fenomeno dell'industria 4.0, si inizia a parlare di I.A. anche al di fuori dei laboratori in cui essa per lungo tempo era stata confinata. Essa entra così silenziosamente, quasi inavvertita, nella vita quotidiana delle persone, fino a plasmare, addomesticare e spesso ottundere le loro menti, nella totale assenza di autocoscienza e di regolazione giuridica.

Occorre, innanzitutto, una dovuta precisazione. La I.A. *in senso lato* costituisce un cerchio al cui interno possono essere incluse numerose applicazioni (RUSSEL 2009). Si pensi, su tutte, alla branca della cibernetica o a quella della robotica, che costituisce una sotto-branca della prima e si occupa di quegli algoritmi intelligenti che operano in un ambiente esterno. Ogni approccio al tema, pertanto, non deve cadere nell'errore di confondere una parte con il tutto.

La I.A. *in senso stretto* si compone di tre elementi: uno proprio della macchina, uno a essa esterno e, per finire, uno indifferentemente interno o esterno alla macchina. Essi sono l'*algoritmo*, l'*informazione* e la *memoria*.

Ciò è vero con riferimento a ogni tipo di applicazione intelligente e trova riscontro nelle definizioni più diffuse di I.A., che tuttavia non prendono sempre in considerazione tutti e tre gli elementi[1].

1 Si veda Relazione del Parlamento europeo, recante *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, doc. A8-0005/2017, 27 gennaio 2017, p. 22, che tuttavia si occupa limitatamente solo di 'robot intelligenti', secondo cui: "È opportuno stabilire una definizione comune europea di robot autonomo intelligente, comprese eventualmente le definizioni delle sue sottocategorie, tenendo conto delle seguenti caratteristiche: – la capacità di acquisire autonomia grazie a sensori e/o mediante lo scambio di dati con il proprio ambiente (interconnettività) e l'analisi di tali dati – la capacità di apprendimento attraverso l'esperienza e l'interazione – la forma del supporto fisico del robot – la capacità di adeguare il suo comportamento e le sue azioni all'ambiente". Si veda, anche, Executive Office of the President, National Science and Technology Council Committee on Technology, *Preparing for the future of Artificial Intelligence*, October 2016, p. 6, dove viene evidenziato che: "There is no single definition of AI that is universally accepted by practitioners. Some define AI loosely as a computerized system that exhibits behavior that is commonly thought of as requiring intelligence. Others define AI as a system capable of rationally solving complex problems or taking appropriate actions to achieve its goals in whatever real world circumstances it encounters". Vedi anche il recente *discussion paper* dell'Information Commissioner's Office del Governo britannico, *Big Data, artificial intelligence, machine learning*

Infatti, da un punto di vista empirico, l'I.A. è il prodotto di un *algoritmo* in grado di processare e sintetizzare una certa quantità di dati in un tempo inversamente proporzionale alla potenza di calcolo della macchina stessa. Ogni algoritmo di I.A. è poi concepito per svolgere una determinata *funzione*, per raggiungere un certo *output* prestabilito dal programmatore.

Tuttavia, l'algoritmo – *rectius* la stringa di linguaggio che compone l'algoritmo – costituisce solo una componente, forse quella più importante, della I.A.. La seconda componente è data dalla informazione processata. Inutile dire, infatti, che maggiore è la mole dell'informazione processata, più raffinata e, si potrebbe dire, 'intelligente', sarà la risposta che la macchina darà a uno specifico stimolo esterno. Quindi, la soluzione data da una macchina intelligente a un certo problema sarà, in termini probabilistici, tanto più esatta quanto maggiore è l'informazione sulla cui base tale soluzione viene fondata.

Infine, il terzo elemento è dato dalla memoria, che consente l'immagazzinamento d'informazioni. Tale elemento non deve essere sottovalutato nell'analisi del fenomeno, giacché maggiore è l'informazione da processare, maggiore sarà lo spazio fisico o virtuale da impegnare.

L'algoritmo, sotto un profilo giuridico, costituisce un'invenzione, un'opera dell'ingegno e, come tale, assoggettabile alla tutela intellettuale come *intangible asset*. Sul punto, la scienza giuridica, pur nella divergenza di vedute circa il tipo di tutela da accordare al software, sembra essere concorde.

L'informazione in senso ampio, invece, appare difficilmente inquadrabile nell'ambito di una sola definizione giuridica. Ciò è dovuto alla natura composita di un termine che racchiude dati, pubblici o privati (talvolta anche personali o sensibili), fatti e interazioni bilaterali o plurilaterali. Peraltro, è stato sottolineato come il concetto di informazione non vada confuso con quello di dati. I dati di per sé sono privi di significato: lo assumono solo in quanto processati dall'algoritmo (ESPOSITO 2017, BATESON 1972).

---

and data protection, 1 marzo 2017; Government Office for Science, *Artificial intelligence: opportunities and implications for the future of decision making*, 9 November 2016, secondo cui per Intelligenza Artificiale (I.A.) s'intende "the analysis of data to model some aspects of the world. Inferences from these models are then used to predict and anticipate possible future events".

Per finire, la memoria costituisce né più né meno che un magazzino, un luogo dove registrare informazioni. Un luogo che, come ogni spazio (fisico o virtuale), si presta a essere illegalmente violato o alterato. Tale circostanza si salda alle problematiche tradizionali che il nascente filone di studi in materia di *cyber security* sta impegnando da qualche anno ormai la dottrina più attenta.

Quando la macchina intelligente è dotata di un substrato fisico, che le consente di muoversi e interagire col mondo esterno, un ulteriore elemento si aggiunge ai tre che compongono l'intelligenza artificiale. Tale ulteriore elemento è il *corpo* della macchina, che, nelle sue quattro componenti, viene così definita *robot*. Il corpo della macchina, rileva sotto un profilo giuridico, su due piani: da un lato, esso estende gli effetti delle azioni della macchina nel mondo esterno; dall'altro, essa consente l'interazione della macchina con l'uomo e con la realtà fenomenica e soprattutto, in forza di questa interazione, laddove l'algoritmo sia così programmato, *l'apprendimento.*

Sotto questo ultimo profilo, deve darsi conto, peraltro, della tendenza attuale della filosofia della scienza ad ampliare la ricerca verso la c.d. E.A. (l'Empatia Artificiale), ossia quell'area della ricerca robotica impegnata nella costruzione di agenti sintetici dotati di competenze affettive (DUMOUCHEL 2016).

3. L'impatto delle più recenti applicazioni di I.A. sulla *privacy*. Verso un perenne stato di sorveglianza. L'I.A. e le sue molteplici applicazioni incidono sulla *privacy* delle persone in maniera molto più pervasiva rispetto alle precedenti innovazioni tecnologiche. Da un lato, infatti, i più recenti sviluppi compiuti in materia di I.A. hanno facilitato le modalità di acquisizione dei dati e, per l'effetto, la quantità di dati disponibili. Dall'altro, le ultime innovazioni in materia di *data mining*, hanno agevolato la capacità di estrarre dalle informazioni *pattern* rilevanti, incidendo sull'elemento qualitativo dell'informazione.

Quanto al primo profilo, paradigmatica è la progressiva diffusione commerciale di robot, androidi, cyborg e droni intelligenti. Non più confinati al solo settore dell'automazione industriale, i robot oggi sono impiegati per

svolgere le più disparate funzioni: dal trasporto di merci alla ricognizione di territori inospitali, dall'assistenza domestica, alle applicazioni militari, dagli interventi chirurgici, all'assistenza sanitaria. A livello mediatico, grande attenzione è stata prestata alle note *Google cars*, le auto senza guidatore di Google, e ai problemi di regolazione a essi collegati. A livello europeo, proprio la necessità di adattare le norme sulla responsabilità civile alla nuova generazione di robot, dotati di capacità di adattamento e apprendimento, ha condotto all'approvazione della nota risoluzione del Parlamento europeo recante *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*[2].

Per ciò che qui interessa, il progressivo sviluppo della robotica incide sulla privacy, in quanto i robot rendono possibile l'acquisizione materiale di informazioni ulteriori non altrimenti acquisibili con altri mezzi. Difatti, i robot possono raggiungere luoghi inaccessibili all'uomo e sono equipaggiati con sensori e telecamere in grado di registrare tutto ciò che avviene in un dato ambiente. Ryan Calo, a tal proposito, sottolinea come i robot incidano sulla privacy delle persone in tre diversi modi (CALO 2012). In primo luogo, essi consentono la diretta sorveglianza di determinati soggetti (SINGER 2009). In secondo luogo, i robot soprattutto quelli domestici, forniscono delle finestre da cui osservare spazi privati e non accessibili (ZITTRAIN 2008). E infine, lo sviluppo di robot dalle parvenze umane e capaci di interagire a livello sociale con l'uomo potrebbe condurre a più intrusive e sottili invasioni della sfera privata.

In relazione a quest'ultimo punto, infatti, Calo sostiene che una delle funzioni della privacy più diffusa nella letteratura prevalente (WESTIN 1967) sia quella di difendere momenti di intimità, riflessione e finanche solitudine. In questo senso, la sempre maggiore diffusione di robot dalle funzioni più sociali in ambienti domestici rischia di azzerare tali momenti, confermando l'affermazione di H.R. Ekbia secondo cui "computers are everywhere" (EKBIA 2008). A ciò si aggiunge che le sembianze umanoidi di un robot hanno effetto sul modo in cui

2 Relazione del Parlamento europeo, recante *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, doc. A8-0005/2017, 27 gennaio 2017.

le persone fisiche interagiscono nella realtà, sentendosi costantemente sotto giudizio e vivendo in uno stato di perenne eccitazione (CALO 2010; SPROUL 1996).

Ma non occorre correre con l'immaginazione ai robot umanoidi per rendersi conto di come la tecnologia faciliti l'acquisizione di informazioni ulteriori e rilevanti, moltiplicando i rischi per la privacy. Numerosi *devices* indossabili, braccialetti elettronici integrati con scarpe da corsa e applicazioni del nostro *smartphone* consentono il tracciamento delle funzioni biologiche della persona e l'incameramento di una elevata mole di dati sensibili. Sotto il vessillo della semplificazione nell'offerta di servizi, vengono giornalmente raccolti infinite quantità di dati biometrici, che consentono di schedare gli individui, concretizzando quell'immaginario di mondo preconizzato da Latour, caratterizzato da "fragments of intelligence distributed through machines, fragments of machines dispersed through bodies, fragments of organizations morphed into software lines, fragment of codes sticking into institutions, fragments of subjects floating into virtual space" (LATOUR 1995).

Quanto al secondo profilo, occorre far riferimento alle più evolute tecniche di *data mining* e ai recenti algoritmi di *machine learning*[3] e *deep learning*[4]. Questi pongono nuovi e rilevanti problemi per la privacy. Infatti, l'implementazione del *data mining* permette di estrarre informazione da metadati presenti in rete, evidenziando correlazioni e differenze non identificabili dall'uomo ed estraendo informazioni rilevanti da informazioni

3 Il c.d. apprendimento automatico (*machine learning*) viene definito dall'Information Commissioner Office come "the set of techniques and tools that allow computers to think by creating mathematical algorithms based on accumulated data". Si veda, ICO, *Big Data, artificial intelligence, machine learning and data protection*, 1 marzo 2017. Si veda anche Executive Office of the President, National Science and Technology Council Committee on Technology, *Preparing for the future of Artificial Intelligence*, ottobre 2016, che lo definisce come "statistical process that starts with a body of data and tries to derive a rule or procedure that explains the data or can predict future data".

4 Il c.d. deep learning "involves feeding vast quantities of data through non-linear neural networks that classify the data based on the outputs from each successive layer". Si veda, Information Commissioner Office, *doc. cit*.. In senso analogo si esprime l'Executive Office of the President, National Science and Technology Council Committee on Technology, *doc.cit*., secondo cui "Deep learning uses structures loosely inspired by the human brain, consisting of a set of units (or "neurons"). Each unit combines a set of input values to produce an output value, which in turn is passed on to other neurons downstream".

secondarie. Cosi, ad esempio, è stato dimostrato che i vegetariani perdono meno aerei rispetto al resto della popolazione (MAYER-SCHÖNBERGER 2013) o che il tasso di divorzi in Maine è legato all'uso pro capite di margarina[5]. E, in questo senso, la privacy potrebbe essere minacciata dalla non corrispondenza al vero di tali correlazioni.

L'apprendimento automatico, e in particolare il *deep learning*, fondato sulla tecnologia delle reti neurali al fine di replicare il funzionamento del cervello umano, adduce poi un ulteriore grave problema per la privacy. Infatti, gli algoritmi di *machine learning* sono in grado di compiere generalizzazioni a partire da esempi, al fine di svolgere una data funzione. Tuttavia, l'informazione processata diviene parte dell'algoritmo stesso, andando a formare un ulteriore *layer* della rete neurale, che a sua volta processerà ulteriori dati. Ecco, dunque, che tali algoritmi non solo processano dati, ma evolvono con l'esperienza (i.e. con la memorizzazione dell'informazione prima processata). Ed ecco che i dati, non costituiscono più e soltanto materiale grezzo da processare, ma guidano l'apprendimento futuro. Tale "appropriazione" del dato processato, conseguentemente è rilevante per il diritto della privacy.

4. Da "*right to be let alone*" a strumento di regolazione. L'impatto del moderno diritto alla *privacy* sui futuri sviluppi della I.A. La prima elaborazione del diritto alla privacy si deve a Louis D. Bradeis e Samuel D. Warren (WARREN, BRANDEIS 1890), che nel breve saggio intitolato *The Right to Privacy* e pubblicato nell'Harvard Law Journal nel 1890 ne diedero un'accezione negativa quale *right to be let alone*, quale diritto dell'uomo a essere lasciato solo, quale possibilità di scelta di esclusione dal consesso sociale.

Molti anni sono passati da allora e questo particolare significato di privacy ha lasciato il posto a nuove formulazioni normative del suddetto diritto, quale diritto di mantenere il controllo sulle proprie informazioni e,

5 http://www.tylervigen.com/spurious-correlations

conseguentemente, come diritto all'autodeterminazione informativa (RODOTÀ 1991).

Tale passaggio da una connotazione negativa del diritto alla privacy – intesa quale non ingerenza nella sfera privata – a una connotazione positiva – come autodeterminazione e controllo - è coincisa con l'avvento computer (WESTIN 1970) e si ritrova nelle prime formulazioni normative del diritto alla privacy.

Sul solco di questa evoluzione si inserisce la c.d. General Data Protection Reform[6], che in un certo senso costituisce una risposta all'aumento esponenziale dei *big data* e ai progressi tecnologici avvenuti in materia di *data mining*, I.A. e robotica. Esso, in questo senso, introduce nuovi principi e disposizioni volti a potenziare le garanzie di un controllo effettivo delle persone sui propri dati personali.

Il controllo viene assicurato da penetranti obblighi posti in capo a chiunque proceda al trattamento dei suddetti dati[7] e da severe sanzioni in caso di inosservanza degli stessi obblighi[8]. Al contempo, al controllo viene affiancato il riconoscimento normativo della "piena disponibilità" dei propri dati personali in uno con la presa di coscienza del loro valore economico. Diritti come quello di rettifica (art. 16), quello alla cancellazione dei dati (art. 17), quello di limitazione di trattamento (art. 18) o quello alla portabilità dei dati (art. 20) delineano un rinnovato diritto alla protezione dei dati personali che poggia su un sostanziale *empowerment* del consumatore rispetto a tutti quegli operatori il cui modello di business poggia sul trattamento di dati personali.

La privacy, da questa prospettiva, diviene lo strumento di una regolamentazione economica, sovrapponendosi alla disciplina della concorrenza[9].

6 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati.
7 Cfr. Capo IV.
8 Cfr. Capo VIII.
9 Basti pensare a tal riguardo al diritto alla portabilità dei dati (art. 20), cui è sottesa, secondo il Garante della Privacy, "L'aspettativa…che, oltre ad ampliare il margine di controllo dei consumatori impedendo forme di 'lock in' tecnologico…promuova l'innovazione e la

Non è infatti un caso che, poco più di un anno fa, le autorità della concorrenza francese e tedesca abbiano formalmente adottato un documento di studio congiunto sugli effetti anticoncorrenziali derivanti dalla raccolta, dal trattamento e dall'utilizzazione dei dati[10].

In questo senso, da baluardo contro l'altrui intrusione nella sfera privata, la privacy diviene dapprima diritto alla libera autodeterminazione della persona e all'autenticità e veridicità dell'informazione, per trasformarsi in strumento di regolazione economica.

In quanto tale, la protezione dei dati personali nella sua moderna accezione, entra in scelte di politica economica e pone innumerevoli implicazioni in relazione all'innovazione tecnologica. Ciò è di particolare evidenza nel caso della I.A..

Volgendo, infatti, l'attenzione ai più moderni algoritmi di *machine learning* e *deep learning*, ci si accorgerà di come questi abbisognino di grandi quantità di dati per funzionare. Si pensi, ad esempio, all'algoritmo usato da Uber per prevedere in modo accurato le abitudini di viaggio degli utenti o categorie di utenti o all'algoritmo di Amazon che offre esperienze di acquisto sempre più personalizzate per l'utente. Si pensi agli algoritmi di riconoscimento vocale e agli assistenti virtuali degli *smartphones* o GPS e agli algoritmi utilizzati dai maggiori motori di ricerca. Ma si pensi ancora alla piattaforma Watson Health, che analizza milioni di dati sanitari per addivenire a diagnosi sempre più precise e trattamenti sanitari più efficaci. Tutti questi dati rientrano, infatti, a pieno titolo nella definizione di "dati personali", elaborata dal nuovo regolamento europeo e incentrata sul perno della riconducibilità, diretta o indiretta, dei dati stessi alla persona fisica[11]. Conseguentemente, al loro trattamento dovranno applicarsi tutte le disposizioni del Regolamento (UE) 2016/679.

---

condivisione di dati personali fra titolari del trattamento in piena sicurezza e sotto il controllo dell'interessato". Cfr. Garante della Privacy, gruppo di lavoro articolo 29 in materia di protezione dei dati personali, Linee-guida sul diritto alla "portabilità dei dati", adottate il 13 dicembre 2016.

10 Si veda il Report congiunto della Autorité de la concurrence e della Bundeskartellen, *Competition Law and Data*, 10 maggio, 2016.

11 I "dati personali", nell'ambito del nuovo regolamento UE, sono definiti in senso ampio come "qualsiasi informazione riguardante una persona fisica identificata o identificabile (…) direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un

4.1 La trasparenza sull'uso dei dati in una "*black box society*". La relatività di un concetto. Nel febbraio 2017, il Tribunale Amministrativo Regionale per il Lazio, annullava una nota ministeriale, con la quale il Ministero dell'Istruzione (MIUR) denegava l'accesso all'algoritmo usato per gestire i trasferimenti interprovinciali dei docenti della scuola primaria e d'infanzia. La sentenza, accolta con grande clamore mediatico, costituisce l'atto finale di una vicenda cominciata più di un anno prima, quando diversi insegnanti iniziarono a lamentare inspiegabili trasferimenti presso sedi scolastiche a diversi chilometri distanti dalla propria residenza. Di fronte alla richiesta pervenuta di rendere pubblici i codici sorgente dell'algoritmo stesso, il MIUR rispondeva dapprima fornendo una generica descrizione della procedura informatica seguita e, poi, negando l'accesso richiesto in ragione *inter alia* della tutela del software quale opera dell'ingegno e della non assimilabilità dello stesso a un atto amministrativo. Nel disattendere le suddette argomentazioni, il TAR Lazio finiva per ordinare l'accesso all'incriminato algoritmo dopo averlo qualificato come "atto amministrativo informatico"[12].

La descritta vicenda mette in luce come algoritmi intelligenti dominino la vita di tutti i giorni e prendano decisioni che finiscono per impattare notevolmente sulla sfera dell'individuo: gli algoritmi sollecitano le decisioni di acquisto e i nostri gusti musicali o cinematografici, decidono il percorso più breve per guidarci da un punto A a un punto B, guidano le decisioni d'investimento finanziario e determinano i cambi tra valute reali e finanche criptovalute. Frank Pasquale (PASQUALE 2015), nel mirabile volume intitolato *The Black Box Society*, descrive una società dove l'informazione e la conoscenza, che costituiscono la quintessenza del potere (BALKIN 2008), sono appannaggio di pochi, schermati da *trade secrets* e disponibili solo agli *insiders*.

numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o piu elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale" (art. 4, comma 1). Si noti, inoltre, che rispetto alla precedente direttiva 95/46/CE, il regolamento aggiunge nel corpo della definizione il riferimento anche a "quei dati relativi all'ubicazione" e a un generico "identificativo online", estendendone oltremodo il perimetro.

12 TAR Lazio, Sede di Roma, sez. III^, 14.2.2017, n. 3769.

Dietro la promessa della tecnologia di predire il futuro attraverso la devoluzione di complessi calcoli statistici a macchine dalla sempre più elevata capacità computazionale, si cela il rischio di una società in cui complesse scelte di policy e valutazioni del rischio sono devolute a processi automatizzati non intellegibili. Sistemi reputazionali e complessi algoritmi di calcolo, guidano la finanza e il commercio globale, sfuggendo all'accesso e alla comprensione dei regolatori e minacciando la privacy, la dignità e la libertà dei singoli. Big data e intelligenza artificiale costituiscono i capisaldi di una siffatta società dove mai il conflitto tra innovazione tecnologica e privacy è stato più netto.

A tal riguardo, il nuovo regolamento europeo, come si è avuto modo di accennare, introduce disposizioni che cercano di rendere più trasparente il trattamento dei dati attraverso algoritmi di I.A.. Questi, infatti, siano essi ascrivibili a modelli di intelligenza artificiale debole o forte, processano dati, che rientrano a pieno titolo nella nozione di "dati personali" fornita dal nuovo regolamento. Ecco, dunque, che il "trattamento" che di tali dati viene fatto attraverso l'algoritmo diviene rilevante per il moderno diritto della privacy, configurando una specifica fattispecie di "trattamento automatizzato".

All'articolo 1, il regolamento europeo annovera tra i principi applicabili al trattamento dei dati "la liceità, correttezza e *trasparenza*". Alla trasparenza sono poi dedicate due sezioni del capo 1, la prima intitolata "trasparenza e modalità" e la seconda "informazione e accesso ai dati". Più nello specifico, è previsto che il titolare del trattamento adotti misure appropriate per fornire all'interessato tutte le informazioni e comunicazioni "relative al trattamento in forma coincisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro" (art. 12). Le informazioni da fornire riguardano sia quei dati personali che siano raccolti presso l'interessato (art. 13), sia quei dati che siano raccolti altrove (art. 14).

È poi riconosciuto il diritto di accesso dell'interessato, che si sostanzia nel "diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento e, in tal caso, di ottenere l'accesso ai dati personali".

Tale complesso di disposizioni delinea un sistema diretto a dare attuazione alla trasparenza, intesa come intellegibilità e comprensibilità del trattamento. Non a caso, già nel considerando n. 39, si evince che "il principio di trasparenza impone che le informazioni e le comunicazioni…siano facilmente accessibili e *comprensibili*". Eppure, il regolamento, non chiarifica cosa debba intendersi per "comprensibili" e come debba essere interpretato un concetto cosi relativo, destinato a variare da un punto di vista soggettivo e oggettivo. Del tutto intuitivamente, infatti, ciò che è comprensibile a un ingegnere informatico non lo è ugualmente a una casalinga o a un avvocato. E, altrettanto intuitivamente, una cosa è comprendere in astratto le finalità del trattamento, altra cosa è comprendere in che modo tali finalità sono perseguite, ad esempio per sindacarne gli *outputs*. Ancora, una cosa è comprendere che esista un processo di profilazione, altra cosa è comprendere come un profilo sia stato elaborato, nonché "quelle informazioni significative sulla logica utilizzata" (art. 14, comma 2, lett. g)) necessarie per eventualmente sindacarne la corrispondenza al vero.

Come la vicenda dell'incriminato algoritmo del MIUR ha messo in luce, esistono diversi gradi di comprensibilità ma, laddove siano in contestazione le scelte operate da complessi algoritmi di calcolo che intaccano su diritti e libertà dei singoli, questa deve essere assicurata nella forma più ampia possibile, che finisce per coincidere con l'accesso ai codice sorgente dell'algoritmo.

Si giunge qui al nodo del problema, che diventa particolarmente spinoso quando il trattamento dei dati sia svolto per il tramite di algoritmi di I.A. protetti in qualità di opere dell'ingegno o tutelati per il tramite di *trade secrets*. È difatti di tutta evidenza il conflitto latente tra *data protection* e proprietà intellettuale in tutti quei casi in cui complessi algoritmi di calcolo processano dati personali. Tra le limitazioni all'accesso alle suddette informazioni (art. 23), infatti, non figura la necessità di tutelare il segreto industriale e aziendale, eppure, al considerando n. 63, si evince che "(il diritto di accesso) non dovrebbe ledere i diritti e libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti di autore che tutelano il software". Nel silenzio del

legislatore europeo, spetterà probabilmente al neoistituito comitato europeo per la protezione dei dati personali sciogliere il dilemma di quale dei due valori debba prevalere.

4.2. Il *trade-off* tra tutela dei dati personali e libero accesso alla conoscenza. Nel lontano marzo 1991 la Stanford Universiy ospitava il primo simposio mondiale sulle problematiche poste dall'intelligenza artificiale (I.A.) per il diritto della proprietà intellettuale. L'iniziativa ebbe ampia risonanza non soltanto per la presenza di eminenti personalità della Silicon Valley e grandi studiosi della materia, ma soprattutto per il fatto di essere stata organizzata dalla World Intellectual Property Organization (WIPO).

Tra le varie criticità che emersero in quella sede, una in particolare appare cruciale per il presente lavoro. In particolare, Andy Johnson-Laird si chiedeva:

> *"What about the facts used to train the neural network? If they are facts, can they be protected? Well you can say, I have organized them in a particular way, I would like to protect them as a compilation? But the networks learned better when you randomized the facts. How could you protect those? I talk here about the ownership of knowledge, and I know, under the law, ownership and autorship are fairly close together"*[13].

In altri termini, la riflessione che l'ingegnere aveva aperto riguardava proprio la proprietà (c.d. *ownership*) di tutti quei "fatti" utilizzati per affinare la capacità predittiva di un qualsiasi algoritmo intelligente. Infatti, se già al tempo era indubitabile che un algoritmo costituisse un'opera intellettuale, molto più controversa appariva la natura giuridica dell'informazione processata e la possibilità di accordare ad essa una qualsivoglia tutela autoriale. Dalle parole di Johnson-Laird, tuttavia, sembrava chiaro che l'algoritmo da solo fosse una

13 WIPO Worlwide symposium on the Intellectual Property Aspects of Artificial Intelligence, Stanford University (California), United States of America, 25 – 27 marzo, 1991 (ftp://ftp.wipo.int/pub/library/ebooks/wipopublications/wipo_pub_698e.pdf).

semplice scatola vuota (BALKIN, 2017), destinata a essere riempita dall'informazione e che la "conoscenza" fosse la risultante delle due componenti.

Questa relazione simbiotica tra algoritmo e informazione implica due cose: in primo luogo, se l'informazione si compone in massima parte di dati che rientrano nell'accezione di "dati personali", la *data protection* viene a sovrapporsi con la tutela della proprietà intellettuale, nel senso che i dati personali divengono parte integrante dell'originaria stringa di linguaggio di programmazione dell'algoritmo; in secondo luogo, per ciò che qui interessa, se i dati costituiscono la risorsa essenziale per lo sviluppo di algoritmi di I.A., sussiste un *trade-off* tra le opportunità connesse a un libero sfruttamento dei dati e i limiti derivanti dal riconoscimento di un elevato livello di *data protection*, proprio come sussiste un *trade-off* tra libero accesso alla conoscenza e il riconoscimento di diritti di privativa sull'algoritmo. Infatti, in un ecosistema in cui i dati sono il sostrato essenziale della "conoscenza", qualsiasi limitazione al loro accesso, anche se strumentale alla tutela di ulteriori diritti, si traduce in una limitazione della conoscenza stessa, intesa quale bene comune.

4.2.1 Segue. Un insanabile conflitto: la qualificazione dei dati. La sopradescritta dualità conflittuale tra protezione dei dati personali e accesso alla conoscenza trova la sua ragione giustificativa nella diversa qualificazione giuridica che viene attribuita ai dati.

In letteratura è stato rilevato come esistano molteplici definizioni di dati, in relazione a diversi contesti (ZENO ZENCOVICH 2016). I dati, sebbene siano qualificati dalla teoria economica come beni pubblici non rivali e non consumabili (SAMUELSON 1954), sono al contempo *commodities* scambiabili sul mercato.

Con specifico riferimento ai dati personali, poi, il concetto di *commodity*, già in passato, aveva diviso la dottrina prevalente. Da un lato vi erano coloro che consideravano i beni personali veri e propri beni giuridici, di cui l'interessato dispone e che può trasferire mediante la manifestazione del consenso

(MORMILE 2006; MANES 2001; OLIVO 2002). Dall'altro vi erano, invece, coloro che contestavano tale reificazione, sulla scorta del rilievo secondo cui l'interessato, attraverso la manifestazione del consenso al trattamento, non perde il alcun modo la titolarità e il controllo di tali dati (ORESTANO 2003). La *querelle* dottrinale finiva quindi per riguardare la natura del consenso, quale atto negoziale dispositivo di un bene giuridico o, alternativamente, atto meramente autorizzativo di un'invasione nella propria sfera giuridica ad opera di terzi. Nel primo caso, la funzione dispositiva del consenso sarebbe stata tendenzialmente incompatibile con un qualsivoglia atto contrario di revoca, rispondendo all'esigenza di assicurare una certa stabilità al sinallagma contrattuale; nel secondo caso, invece, la revoca sarebbe strumentale ad assicurare la protezione dell'identità personale dell'individuo, rispetto a trattamenti dei dati personali consentiti nel passato.

Siffatta questione è stata risolta dal legislatore europeo, che, a prima vista, sembra aver confermato il secondo indirizzo[14]. Il nuovo regolamento europeo, infatti, nell'attribuire una serie di diritti al titolare dei dati personali oggetto di trattamento, attribuisce all'interessato la facoltà di disporre pienamente dei propri dati, a prescindere dal *consenso* prestato o dal *contratto* sottoscritto con il titolare del trattamento. Tanto è vero che, all'art. 7 comma 3, è stabilito che "L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento (…) Il consenso è revocato con la stessa finalità con cui è accordato". La revoca del consenso, tuttavia ha efficacia solo *pro futuro* e "non pregiudica la liceità del trattamento basata sul consenso prima della revoca".

In ultima analisi, dalla prospettiva del diritto della privacy, i dati personali giammai dovrebbero essere giuridicamente assimilati a una *commodity*. Sembra, dunque, determinarsi un'irreparabile frattura tra la concezione

14 Nello stesso senso di escludere la natura di beni dei dati personali, si è, inoltre, recentemente espresso l'European Data Protection Supervisor (EDPS), opinion 4/2017, 14 marzo 2017, secondo cui occorrerebbe evitare l'uso del termine "*data as a counter-performance*", in quanto "There might well be a market for personal data, just like there is, tragically a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation".

economica dei dati personali e quella giuridica fatta propria dal microcosmo legislativo della *data protection*.

4.2.2 Segue. La rimozione dei dati usati per allenare l'algoritmo, tra diritto alla cancellazione e *machine learning*. È in questo scenario che occorre contestualizzare le implicazioni del nuovo regolamento europeo sui futuri sviluppi delle applicazioni di I.A.. Tra di esse, sembra centrale affrontare quello che parrebbe il punto di emersione di questo inconciliabile conflitto tra le suddette opposte concezioni, vale a dire il rapporto tra algoritmi di *machine learning* e diritto alla cancellazione, anche detto "diritto all'oblio".

Quest'ultimo, portato alla ribalta mediatica dal famoso caso *Google Spain*[15], viene inteso, nella positivizzazione operata dal legislatore europeo, come quel "diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo". Le basi filosofiche del diritto all'oblio affondano nel pensiero di Heiddeger e Ricoeur: il rapporto col passato, particolarmente in Ricoeur, si fonda su una relazione attiva, che permette una rielaborazione del senso proprio di vicende già verificatesi. Se una certa dose di dimenticanza è quasi necessaria per portare a compimento il processo di rielaborazione del passato individuale, ciò non vuol dire che il soggetto debba cancellare le tracce dei fatti accaduti. Potrà, invece, attribuire loro un nuovo significato che sarà condivisibile con la comunità. In questo senso l'identità personale implica necessariamente il confronto con la comunità nel momento in cui essa accede e conosce quel passato. Il potere di ricostruzione del passato del singolo deve saper coesistere con quello che gli altri hanno di poter accedere alle informazioni tipiche di un passato condiviso, di un sapere comune.

Del c.d. diritto all'oblio comunque sono state date diverse e talvolta contrastanti interpretazioni, come "right not to disseminate" (PIZZETTI 2013), ossia diritto alla non divulgazione dei propri dati, come "right to contextualise"

15 Corte di Giustizia UE, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos*, causa C-131/12.

(PIZZETTI 2013), vale a dire diritto alla contestualizzazione dei dati nel tempo e come "right to reinvention" (SOLOVE 2011), come diritto cioè a reinventare il presente disancorandolo dal passato. Tutte le suddette definizioni sono accumunate da un'interpretazione del diritto all'oblio quale diritto funzionale alla costruzione e allo svolgimento della propria identità personale, in una dialettica che vede compartecipe anche l'"altro", appunto il contesto sociale dal quale è impossibile prescindere.

All'opposto estremo, in una relazione conflittuale, stanno invece gli algoritmi di *machine learning*, programmati per sintetizzare attraverso complessi calcoli statistici i dati a disposizione e memorizzarne gli *output* essenziali. In questo senso, l'algoritmo processa una quantità di dati di gran lunga superiore rispetto a quella di cui è a conoscenza il singolo. Esso evidenzia correlazioni e differenze tra metadati ed è in grado di estrarre informazioni rilevanti da informazioni secondarie.

La memoria consente l'apprendimento, che nei casi di apprendimento senza rinforzo, è al di fuori del dominio del programmatore. I dati vengono acquisiti, raffinati, memorizzati e utilizzati come mattoni per costruire, attraverso la loro aggregazione in *cluster* uniformi, l'intelligenza stessa dell'algoritmo. Pur se inaccessibili attraverso l'indicizzazione dei motori di ricerca i dati continuano, dunque, a esistere all'interno di una onnipresente "memoria algoritmica" (ESPOSITO 2017)[16].

Si assiste, in altri termini, a un processo di "appropriazione" e "rielaborazione" dell'informazione da parte della macchina, divenendo l'informazione componente essenziale dell'algoritmo stesso. La relazione che si istaura tra dati e algoritmo è biridezionale. Da un lato, l'algoritmo processa e interpreta i dati che compongono l'informazione, dall'altro, l'informazione fa evolvere l'algoritmo, diventando essa stessa componente dell'algoritmo.

La moderna *data protection*, tuttavia, sembra non prendere direttamente in considerazione questo rapporto nella sua totalità, fermandosi alla disciplina

16 Altri autori hanno affermato che l'algoritmo usa "data exhaust" o "data shadows", generati indirettamente dagli individui sul web (KOOPS 2011).

della “raccolta” e del “trattamento dei dati” e occupandosi di tutelare la persona solo contro pratiche di *profiling*[17] e contro quelle scelte adottate sulla base di processi di trattamento dati automatizzata[18]. Ma *quid iuris* nel caso in cui i dati personali fuoriusciti dalla sfera di dominio dell’individuo, continuino a essere utilizzati al di fuori del contesto nel quale erano forniti o si trasformino addirittura in tanti ulteriori *layer* di una rete neurale usata da un algoritmo di I.A..?

Siamo qui giunti al centro della questione. Il diritto alla cancellazione dei dati potrebbe essere interpretato estensivamente nel senso di spezzare il nesso tra passato e presente, anche in relazione all’informazione fatta propria da un algoritmo di *deep learning*? O fuoriesce, piuttosto, dallo scopo originario di tale diritto una siffatta tutela, dovendosi piuttosto affrontare il problema di una siffatta “appropriazione” dei dati esclusivamente dalla prospettiva del diritto della proprietà intellettuale? In altri termini, senza voler scendere nella questione dell’inquadramento giuridico di un algoritmo di *deep learning*, viene da chiedersi se la memoria che suddetta entità ha dell’informazione possa impattare sulla costruzione della identità del singolo nel contesto sociale, ovvero se il fatto che l’informazione sia priva di significato per la macchina escluda in *nuce* tale eventualità.

La risposta non è poi cosi scontata, laddove si osservi che se l’algoritmo è incosciente e al contempo intellegibile per la generalità delle persone, non lo è per gli *insiders* che lo hanno creato, i quali ben potrebbero, compiendo il percorso inverso, ricondurre l’informazione processata agli originali “dati personali”. Inoltre, la profilazione operata dell’algoritmo, attraverso un’autonoma reinterpretazione dei dati personali processati (AMOORE 2015), potrebbe alimentare il sentimento di essere categorizzati, schedati, etichettati, finendo per riflettersi sull’identità del singolo.

17 Cfr. Art. 4, comma 1, n. 4 del Regolamento (UE), ai sensi del quale deve intendersi per profilazione “qualsiasi forma di trattamento automatizzato di dati personali per valutare determinati aspetti personali relative a una persona fisica…”.
18 Cfr. Art. 22 del Regolamento (UE), ai sensi del quale “L’interessato ha diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significamente sulla sua persona”.

E il problema, a questo punto, riguarderebbe l'implementazione e l'*enforcement* di un tale diritto (CUSTERS 2016), posti gli elevati costi e tempi connessi all'individuazione dell'uso che dei dati personali viene fatto da macchine intelligenti.

5. Osservazioni conclusive. Fino ad oggi, nessuna innovazione tecnologica aveva messo in discussione così nel profondo il diritto della privacy come l'intelligenza artificiale. Tra i due, si è visto, s'istaurano complesse ingerenze reciproche. Infatti, da un lato, la I.A. nelle sue più moderne applicazioni moltiplica le possibilità di lesione della sfera individuale del singolo. Dall'altro, la privacy, nella sua moderna accezione di *data protection*, è divenuta non più e soltanto strumento a salvaguardia della propria sfera personale, ma strumento di regolazione economica.

Il legislatore europeo, in questo senso, ha adottato una disciplina che ha la presunzione di rafforzare il controllo del singolo sull'utilizzo dei propri dati e di estendere oltremodo il perimetro del suo ambito di applicazione.

Tale approccio, tuttavia, appare fortemente deficitario laddove si scontra con gli ultimi sviluppi in materia di I.A.. Da un lato, appare ingenua la pretesa di assicurare la trasparenza e il consenso informato a ogni tipo di trattamento, in un prevedibile scenario caratterizzato dall'uso sempre più estensivo di algoritmi non intellegibili dall'essere umano. Dall'altro, data l'assoluta centralità dei dati nello sviluppo di algoritmi di apprendimento automatico, deve sottolinearsi l'emersione di complesse sovrapposizioni tra *data protection* e proprietà intellettuale. Infatti, se i più moderni algoritmi di *machine learning* ottengono informazioni rilevanti a partire dai dati e al tempo stesso evolvono attraverso l'analisi di tali informazioni, sussiste un *trade-off* tra le opportunità connesse a un libero sfruttamento dei dati e i limiti derivanti dal riconoscimento di un elevato livello di *data protection*. Tale *trade-off* origina dalla diversa qualificazione della natura dei dati che, dalla prospettiva del moderno diritto della privacy, non devono considerarsi alla stregua di *commodity* scambiabili sul mercato. Questa diversità di vedute circa la natura dei dati è all'origine di una serie di problemi

quando si tratti di applicare la recente GDPR all'informazione processata da algoritmi di *machine learning*. Infatti, particolarmente critico risulta stabilire se il consenso al trattamento dei dati personali sia stato prestato per tutti gli usi che dei dati vengono fatti dagli algoritmi di *deep learning*. Ma, molto più critico, inoltre, è stabilire se il diritto alla cancellazione dei dati, previa revoca del consenso, possa trovare applicazione in questa materia o se l'"appropriazione" dei dati ad opera di un algoritmo di I.A. sia piuttosto questione del diritto della proprietà intellettuale. In relazione a questo problema, più che mai è necessario adottare una visione unitaria circa la natura dei dati, abbandonando l'approccio a compartimenti stagni che fino ad ora ha caratterizzato l'azione del legislatore e della dottrina. Infatti, in un'epoca dove i dati costituiscono la materia grezza della conoscenza, intaccando ogni settore economico e branca del diritto, lo sforzo del regolatore non può prescindere dall'elaborazione di una definizione comune di dati e da norme che cerchino di anticipare l'emersione di vuoti normativi e insanabili *clash* di discipline.

Riferimenti bibliografici

AMOORE L., PIOTUKH V., *Life beyond big data: Governing with little analytics*, in *Economy and Society*, vol. 44, 2015.

BALKIN J., *The Constitution in the National Surveillance State*, in *Minnesota Law Review*, vol. 93, 2008.

BALKIN J., *The Three Laws of Robotics in the Age of Bid Data*, in *Ohio St. L.J.*,vol 78., 2017.

BATESON G., *Steps to an Ecology of Mind*, Ballantine Books, New York, 1972.

CALO M. R., *Robots and Privacy*, in P. LIN, K. ABNEY, G. A. BEKEY (a cura di), *Robot Ethics: The Ethical and Social Implications of Robotics*, MIT Press, London, 2012.

CALO M. R., *People can be so fake: A new dimension to privacy and technology scholarship*, in *Penn. St. L. Rev.*, vol. 114, 2010.

CHEMERINSKY E., *Rediscovering Brandeis's Right to Privacy*, in *Brandeis L.J.*, vol. 45, 2007.

CUSTERS B., *Click here to consent forever: Expiry dates for informed consent*, in *Big Data & Society*, vol. 2, 2016.

DUMOUCHEL P., DAMIANO L., *Vivre avec les robots, Essai sur l'emphaties artificielle*, Seuil, 2016.

ESPOSITO E., *Algorithmic memory and the right to be forgotten on the web*, in *Big Data & Society*, 2017.

EKBIA H. R., *Artificial Dreams*, Cambridge University Press, New York, 2008.

GAVISON R., *Privacy & The Limits of Law*, in *Yale L.J.*, vol. 89, 1980.

KOOPS J. B., *Forgetting footprints, shunning shadows. A critical analysis of the right to be forgotten in big data practice. Scripted* 8 (3), 2011.

LATOUR B., *Social theory and the study of computerized work sites,* in W. J. ORLINOKOWSKI, G. WALSHAM (a cura di), *Information Techinology and Changes in Organizational Work*, Chapman and Hall, London, 1995.

MANES P., *Il consenso al trattamento dei dati personali,* Padova, 2001.
MAYER-SCHÖNBERGER V., CUKIER K., *Big Data. A Revolution That Will Transform How We Live, Work, and Think*, London: Murray, 2013.
MORMILE L., *Lo Statuto giuridico die dati personali*, in R. PANETTA (a cura di*), Libera Circolazione e protezione dei dati personali*, Giuffè, 2006.
OLIVO F., *Dati personali e situazioni giuridiche soggettive*, in *Giust. Civ*. vol. 4., 2002.
ORESTANO A., *La circolazione dei dati personali*, in R. PARDOLESI (a cura di), *Diritto alla Riservatezza e circolazione dei dati personali*, Giuffè, 2003.
PASQUALE F., *The Black Box Society, The Secret Algorithms That Control Money and Information*, Harvard University Press, London, 2015.
PIZZETTI F., *Il prisma del diritto all'oblio*, *Il caso del diritto all'oblio*, Torino, 2013.
RODOTÀ S., *Privacy e costruzione della sfera privata, Ipotesi e Prospettive*, in *Pol. Dir.*, 1991.
RUSSELL S., NORVIG P., *Artificial Intelligence: A modern Approach*, England: Pearson, Essex, 2009.
SAMUELSON P. A., *The Pure Theory of Public Expenditure*, in *The Review of Economics and Statistics*, 36, 387 ss, 1954.
SOLOVE D. J., *Speech, privacy and the reputation on the internet*, in M. NUSSBAUM, S. LEVMORE. *The offensive internet: Speech, Privacy and the Reputation*, Cambridge MA, MH Harvard U.P., 2011.
SINGER P. W., *Wired for War*, The Penguin Press, New York, 2009.
SPROULL L., *When the Interface is a Face*, in *Human – Computer Interaction*, vol. 11, 1996.
WARREN S. D., BRANDEIS L. D., *The right to privacy*, in *Harvard Law Review*, Vol. 4, No. 5, 1980.
WARWICK K., *Artificial Intelligence – The Basics*, Routledge, 2012.
WESTIN A., *Privacy and Freedom*, New York: Atheneum, 1970.
ZENO ZENCOVICH V., CODIGLIONE G. G., *Ten Legal perspectives on the "Big data revolution"*, in F. Di PORTO (a cura di), *Big data e concorrenza*, vol. 23, Giuffrè, 2016.
ZITTRAIN J., *The Future of the Internet: And How to Stop it*, Yale University Press, New Haven, 2008.