Big Data e diritto: una sfida all'effettività*

Lara Merla

Abstract

Il presente paper, incentrato sulle sfide che interessano il giurista nella nuova società tecnologica, presenta un taglio spiccatamente e volutamente interdisciplinare. Esso cerca di mettere in luce quali sono i problemi e le novità che un operatore del diritto deve fronteggiare per poter mantenere quel grado di supremazia nel forgiare la società che da sempre detiene. Il saggio ambisce a spiegare come l'uso dei c.d. Big Data, da parte dei governi ma anche di tutti gli operatori economici, stia modificando il modo in cui ciascuno di noi agisce e viene "percepito" all'esterno. Si è voluto altresì porre l'accento sulle carenze della legislazione nazionale ed europea in materia di protezione dei dati personali e da ultimo si è tentato di offrire le linee di una *pars construens* di una visone della privacy concepita non solo e non più come diritto soggettivo del singolo ma come diritto "sociale" ossia come bene comune.

This paper focuses on the challenges facing the jurist in the new technology society. It aims to highlight the problems and the novelties that a lawyer has to face to maintain the supremacy in determining the society. It attempts to explain how the use of Big Data by States and private companies is changing the way each of us acts and is perceived from the outside. It also underlines the failings of national and European legislation about protection of personal data and, last but not least, tries to offer a sort of *pars construens* of a common privacy vision and not only as an individual right.

Sommario

Keywords

privacy - Big Data – giurista – profilazione - bene comune

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco"

Introduzione

Il presente elaborato discute la faticosa resilienza del diritto di fronte ai cambiamenti tecnologici in corso. Propongo qui i preliminari di un progetto ambizioso. Infatti, da un lato il diritto deve farsi carico di fenomeni tecnologicamente nuovissimi come la raccolta e lo sfruttamento dei Big Data e lo sviluppo dell'Intelligenza Artificiale; dall'altra parte ciò deve avvenire tenendo conto della perdita di autorevolezza del giurista di fronte ad altre figure professionali capaci di maneggiare il linguaggio informatico: alludiamo al *coder* o programmatore[1].

Dopo una breve premessa sulla trasformazione materiale delle condizioni del presente volta a mostrare come gli esiti della discussione risalente e classica sui limiti del formalismo ci consentono di affrontare a mente sgombra i temi nuovi, il secondo paragrafo affronterà il complesso rapporto fra raccolta ed elaborazione dei Big Data ed i diritti fondamentali sempre più minacciati dalle tecnologie dell'informazione e della comunicazione (ICT) applicate ad ogni aspetto della vita quotidiana. Sarà introdotta una prima panoramica della dimensione collettiva che costituisce la matrice dei Big Data e di come essa possa coniugarsi con la struttura individualistica del diritto occidentale fondato sulla costruzione del diritto soggettivo.

Nel terzo paragrafo ci occuperemo del diritto alla privacy alla luce del regolamento (UE) 679/2016 evidenziando un assetto normativo non sempre in grado di raggiungere lo scopo, proprio in virtù del suo legame strutturale con il soggetto di diritto titolare della potestà di prestare il consenso[2].

In chiusura, (quarto paragrafo) indicheremo quelle che pensiamo essere le grandi linee di futuri approfondimenti volti ad illustrare una concezione nuova del diritto alla privacy, presa in considerazione in qualche modo dai legislatori europei in sede di discussione del regolamento (UE) 679/2016 ma poi non seguita nell'approvazione definitiva. Si tratta dell'elaborazione di un concetto di privacy come bene comune digitale capace di offrire una risposta istituzionale collettiva e transnazionale ad una domanda sociale di sicurezza informatica ed informativa prodotta da una sfida tecnologica a sua volta collettiva e transnazionale che mette in scacco il dualismo fra Stato e individuo portatore di diritti.

1. La crisi dell'effettività del diritto

Non è questa la sede per un'analisi anche solo accennata della condizione del presente. Si può dare per assodato che il diritto sia oggi "sconfinato"[3] e che lo Stato sovrano abbia largamente perduto il monopolio sulle sue fonti. Ciononostante, lo spazio del

[1] Si veda per una prima panoramica L. Lessig, *Code and other laws of cyberspace,* New York, 1999.

[2] Si veda, per una prima panoramica circa le problematicità che pone il "consenso" una recente pronuncia del Garante Privacy dal titolo: *Operatori telefonici: continua l'attività di controllo del Garante privacy, sanzione a Wind per 17 milioni di euro e a Iliad per 800 mila euro*, reperibile in *gdpd.it*.

[3] Si veda per tutti M. R. Ferrarese, *Il diritto sconfinato. Inventiva giuridica e spazi nel mondo globale,* Bari-Roma, 2006.

giuridico viene ancora gelosamente mantenuto separato da quello del politico e dell'economico dalla riflessione dominante[4].

Il giurista positivista costruisce una strategia di auto-legittimazione fondata sulla scansione artificiale di un medesimo fenomeno materiale quale quello del modo in cui un gruppo sociale si governa. Egli partecipa da protagonista alla regolamentazione del sapere accademico[5] ma consegna al *politologo* la fase precedente la validità formale della norma (sono i politologi a studiare i processi parlamentari e prima ancora quelli elettorali) e al *sociologo* lo studio dei suoi effetti concreti. Fra il prima e il dopo si colloca il giurista, forte di tecniche ermeneutiche in cui formalismo e realismo si confrontano in uno spazio protetto dalle pulsioni delle condizioni politiche materiali. Il dibattito sull'effettività del diritto e soprattutto sui suoi legami con questioni diverse ma correlate come la legittimità e la validità si articola in questo spazio. Qui si confrontano alcuni fra i più importanti studiosi del XIX secolo che nell'ambito della tradizione giuridica occidentale si sono posti il problema dell'efficacia di un diritto (im)posto dall'alto. Fra gli eroi eponimi di questi dibattiti che coinvolgono la questione stessa dei confini del diritto: Santi Romano, Carl Schmitt, Hans Kelsen, Herbert Hart. Tutti costoro, storicizzati al punto dall'esimerci perfino dall'offrire una bibliografia ancorché sommaria sul loro pensiero, si interrogano a fondo sull'effettività della norma. Tale requisito, direttamente connesso nello spazio della loro riflessione, all'efficacia ed alla validità, diviene ancor più cruciale oggi con l'avvento di una tecnologia globale non governabile nei limiti della statualità.

Ai nostri fini basta registrare che i maestri del positivismo si interrogano sulla commistione tra ordinamenti ed in particolare tra il diritto statale e quello internazionale che, come noto, annovera tra le sue fonti proprio la consuetudine, ossia comportamenti fattuali ripetuti nel tempo ai quali la comunità riconosce carattere di obbligatorietà. È chiaro che la questione dell'effettività risulta quanto mai condizionata dalla dimensione transnazionale (o trans-statuale) del diritto, la quale costituisce la sfida più complessa del presente rispetto al periodo storico in cui operavano i maestri del positivismo giuridico in tutte le sue forme. In più, la dimensione transnazionale si fonda oggi su una trasformazione tecnologica delle connessioni globali semplicemente impensabile ai loro tempi.

La fonte consuetudinaria transnazionale, di primaria importanza oggi, ci permette di affermare che, con l'avvento delle nuove tecnologie, il diritto sia ancora in grado di plasmare la società solo se effettivamente seguito dai "cittadini globali" (*rectius*: consumatori globali).

Oggi, infatti, a livello giuridico mondiale l'effettività origina dall'alto da assetti transnazionali dotati di autorevolezza e forza cogente[6], capaci di condizionare l'uso delle tecnologie informatiche (ad es. l'Organizzazione Mondiale del Commercio, l'ICANN e il Fondo Monetario Internazionale) oppure dal basso tramite l'operare di movi-

[4] Si veda sulla forza dirompente del globalismo, P.G. Monateri, *Dominus Mundi, Political Sublime and the new World Order*, Oxford, 2018.

[5] Vedi U. Mattei, *Beni comuni. Un manifesto*, Bari, 2011.

[6] Si veda, per una riflessione critica sul mutato rapporto fra il giuridico ed il politico nel mondo globale, P. G. Monateri, *Dominus mundi: Political Sublime and the World Order,* cit.

menti sociali in grado di agire direttamente sulla tecnologia (ad es. Aron Swartz[7] e il suo Guerrilla Open Access Manifesto). Ma non è tutto. Non solo lo Stato, ancora capace di esercizio di sovranità ai tempi di Romano, Kelsen, Schmitt o Hart, risulta oggi spiazzato e in qualche modo subalterno proprio in virtù di una tendenziale inadeguatezza tecnologica delle proprie strutture burocratiche, ma si registra anche una propensione sempre più accentuata a consegnare nelle mani di soggetti privati, per esempio, la stessa sicurezza cibernetica dello stato.
In altre parole, l'ordinamento giuridico statuale si trova a competere con sistemi informativo-normativi con esso concorrenti quando non direttamente conflittuali ed ostili, dotati del grande vantaggio di non doversi curare della legittimità. A ciò si aggiunga che la trasformazione tecnologica che ha accompagnato la globalizzazione dei mercati (utilizzo questo termine per non aprire la questione del rapporto causa/effetto) ha determinato uno squilibrio senza precedenti nel rapporto di forza fra capitale privato e istituzioni pubbliche, nell'ambito del quale la fattualità globale del diritto (in altre parole la consuetudine globale) è quanto mai determinata dalla tecnologia della comunicazione (in mani private) che condiziona o perfino determina i comportamenti individuali. È un mondo della fattualità tecnologica quello che ci circonda, all'interno del quale il giurista positivista, sebbene seduto sulle spalle di giganti, si trova del tutto disorientato.

2. L'(in)effettività delle norme nel mondo governato dai Big Data

È noto che la società tecnologica iperconnessa nella quale viviamo si fonda su una memoria collettiva dettagliata priva di precedenti storici. Miliardi di rapporti che nel passato non lasciavano alcuna traccia o comunque erano dimenticati dopo poco tempo (impattando soltanto su un numero ridotto di persone) lasciano oggi impronte informatiche indelebili che consentono una cooperazione sociale di portata assolutamente globale[8]. Per rendersi conto di ciò basti pensare quanti più dati sulla nostra vita reale conosca il nostro telefono *smart* o la nostra posta elettronica rispetto a noi e soprattutto quanto questi strumenti, salvo casi eccezionali, non dimentichino mai nulla (per scongiurare la perdita di questa memoria noi volentieri trasferiamo le nostre rubriche telefoniche e le nostre chat su potentissime memorie collettive dette cloud che sono organizzate e governate dalle *big tech*). O ancora immaginiamo quanto rimangano per sempre registrati i pagamenti che facciamo con un bancomat o con una carta di credito. Insomma, questi miliardi di miliardi di impronte che noi lasciamo in quel grande spazio informatico che ha preso il nome di infosfera[9] hanno rivoluzionato, come la scrittura prima e la stampa poi, la nostra organizzazione sociale ed è esattamente questo il territorio nuovo, dal quale dipende interamente la nuova organizzazione capitali-

[7] A. Swartz, *Guerrilla Open Access Manifesto,* 2008.

[8] Si veda Y.N. Harari, *Sapiens. Da animali a dèi. Breve storia dell'umanità*, Milano, 2017.

[9] L. Floridi, *Infosfera. Etica e filosofia nell'età dell'informazione,* Torino, 2009.

stica che il giurista si trova a dover calpestare[10]. Un territorio assai diverso e di portata globale ben più di quello pur a sua volta in rapida trasformazione, con cui si dovevano misurare i maestri del passato.

L'incessante e crescente raccolta di dati unita al vertiginoso abbassamento dei costi di elaborazione per il loro utilizzo ha reso le nostre vite orami a disposizione di tutti coloro che, per diversi motivi, ne fanno un business[11].

Pensiamo ai dati che ogni giorno concediamo mediante piattaforme come Twitter, Instagram, Facebook ai nostri amici, colleghi, datori di lavoro e, naturalmente, alle piattaforme stesse.

Ma pensiamo anche agli utilizzi meno "ricreativi" dell'uso dei nostri dati che già da tempo ci fanno temere lo sviluppo di una vera e propria società del controllo, un incubo distopico che oltre quarant' anni fa preoccupava, in Italia, pure Stefano Rodotà. [12]

Si pensi a questo caso occorso poco più di 50 anni fa. Il 24 agosto del 1965 Gloria Placente, una trantaquattrenne del Queens, stava guidando verso Orchard Beach, nel Bronx. In short e occhiali da sole, la donna, sposata, non vedeva l'ora di godersi un po' di riposo in spiaggia. Ma, proprio mentre stava attraversando il ponte di Willis Avenue con la sua Chevrolet Corvair, fu fermata e si ritrovò circondata da una dozzina di poliziotti. C'erano anche un centinaio di reporter pronti ad assistere al lancio della nuova iniziativa del dipartimento di polizia di New York, l'operazione CORRAL (Computer Oriented Retrieval of Auto Lancenists, ossia "reperimento di ladri d'auto guidato da computer").

Quindici mesi prima Placente era passata col rosso e non aveva risposto al mandato di comparizione, un'infrazione che CORRAL stava per sanzionare con un'esemplare punizione potremmo dire tecno-kafkiana[13]. L'operazione era strutturata in questo modo: un'auto della polizia ferma in fondo al ponte trasmetteva la targa delle vetture in arrivo a un operatore, seduto a una telescrivente a chilometri di distanza che la immetteva in un computer il quale cercava la targa in un database di 110.000 vetture rubate o appartenenti a delinquenti noti. Nel caso ci fosse stata corrispondenza, l'operatore avrebbe allertato una seconda vettura di pattuglia all'altra estremità del ponte. Tempo di operazione: 7 secondi.

In confronto allo straordinario equipaggiamento di cui è dotata la polizia oggi, riconoscimento automatico delle targhe, videocamere di sorveglianza, localizzatori GPS, l'operazione CORRAL appare simile alla battuta di caccia di popolazioni neolitiche. Oggi con oltre un miliardo e mezzo di rilevatori *smart* che si collegano automaticamente ai nostri dispositivi cellulari e ad altri oggetti operanti nel cosiddetto Internet delle cose ("IoT"), possiamo immaginare un controllo capillare totale sui nostri spostamen-

[10] Si veda U. Mattei - A. Quarta, *Punto di svolta. Ecologia, tecnologia e diritto privato. Dal capitale ai beni comuni*, Sansepolcro, 2018.

[11] Sul mutamento strutturale determinato da questa riorganizzazione si possono leggere le pagine apologetiche di C. Anderson, *The long tail: How endlesss choice is creating unlimited demand,* New York, 2007. Ancor più interessanti e documentate quelle critiche di J. Lanier, *Who owns the future,* New York, 2014; inoltre per l'uso del termine si veda E. Morozov, *Silicon Valley: i signori del silicio,* Torino, 2017.

[12] S. Rodotà, *Calcolatori elettronici e controllo sociale,* Bologna, 1973.

[13] V. M. Schonberger – K. Kukier, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà,* Milano, 2015.

ti. Il settore automobilistico è emblematico delle trasformazioni in atto[14]; John Elkann, presidente di FCA e Ferrari, ha dichiarato che sono anni che lavora insieme a Google alla fabbricazione di macchine intelligenti, le *self driving cars*; anche Apple sta facendo affari con le macchine a guida autonoma puntando sulla creazione di smartphone e occhiali intelligenti dotati di sensori per analizzare, per esempio, se la vettura è in movimento e se la persona che in quel momento usa il telefono è alla guida oppure no: se entrambe le condizioni si verificassero, il software bloccherebbe la funzione di invio dei massaggi. E poi ancora la Intel e la Ford stanno testando sistemi di riconoscimento facciale che, nel caso non dovessero conoscere il volto del guidatore, non solo impedirebbero all'auto di mettersi in moto, ma ne invierebbero anche una foto al proprietario.

Ma gli utilizzi dei dati sono molteplici e gli usi di polizia sono solo una piccola parte perché notoriamente la *business community* è assai più fantasiosa delle burocrazie poliziesche. Un esempio ci viene offerto dagli spagnoli del teatro comunale Treatreneu di Barcellona. Come molte altre realtà culturali spagnole e non solo, questo teatro si è trovato a fronteggiare un calo dell'affluenza dopo che l'amministrazione comunale, al verde e alla disperata ricerca di entrate aggiuntive per tappare i buchi nel bilancio, ha alzato le tasse sulle vendite dei biglietti dall'8 al 21 per cento.

I gestori della sala tuttavia hanno trovato una soluzione ingegnosa: grazie a un accordo con l'agenzia pubblicitaria Cyranos McCann, hanno inserito nello schienale di ogni poltrona un tablet in grado di analizzare le espressioni facciali di chi sta seduto nella fila posteriore. Secondo il nuovo modello di business, i clienti entrano a teatro gratis, ma devono pagare 30 centesimi per ogni risata riconosciuta dal tablet, con un tetto massimo di 24 euro (pari a 80 risate) a spettacolo. Quindi la soluzione è o non ridere mai, premesso che si riesca, oppure pagare. Il guadagno complessivo per ogni biglietto, a quanto si dice, sarebbe aumentato di 6 euro. Dal punto di vista della Silicon Valley quello appena descritto è un perfetto esempio di innovazione radicale (*disruption*): la proliferazione di sensori intelligenti e connessioni internet crea nuovi modelli di business e flussi di denaro[15]. Ovviamente il vero valore per la *corporation* è la conoscenza intima dei gusti di ciascuno spettatore poi elaborabile in macro-tipologie ed utilizzabili a fini pubblicitari.

Lo scenario appena descritto dovrebbe suscitare nel giurista molti interrogativi su quale ruolo assume il diritto in tutto questo. Nel primo esempio vengono in rilievo sia la natura della prova acquisita che le modalità attraverso le quali è stata acquisita, quesiti che interrogano il processualpenalista e che qui per ragioni di spazio ed opportunità non possiamo approfondire, l'ultimo pone un problema sulla natura dei contratti (*smart* o meno che siano) anche con riguardo agli elementi essenziali e specialmente all' adeguatezza della nozione di consenso come caposaldo moderno dell'istituto. Il requisito dell'accordo fonda e legittima tradizionalmente la stessa autonomia contrat-

[14] S. Palanza, Internet of Thinks, big data e privacy: la triade del futuro, in Documenti IAI (Dipartimento Affari Internazionali), 2016, 3, consultabile in *iai.it*; F. Panetta, Harnessing Big Data &, Machine Learning Technologies for Central Banks, in *bancaditalia.it*.

[15] Y. Benkler, *The Pinguin and the Leviathan: How Cooperation Triumphs over Self-Interest,* Redfern, 2011; Id., *The Political Economy of Commons,* 2003.

tuale. Nel diritto occidentale moderno queste idee già presenti nel giusnaturalismo (ed inserite da Domat nei codici) furono sistematizzate dai giuristi tedeschi romantici che reinventarono le categorie classiche del diritto romano impregnandole dello spirito individualistico sostenuto dal Romanticismo[16]. Venne cioè conferita piena centralità alla volontà e all'autonomia privata, fino al punto di non lasciare più alcuno spazio a quella che veniva definita giustizia commutativa o distributiva, ossia quella realizzata col controllo giurisdizionale sull'equità delle scelte operate dalle parti. Ancora oggi durante le lezioni di diritto privato si insegna allo studente la totale irrilevanza, per il diritto, dei motivi che hanno spinto a contrarre. I contraenti divennero quindi liberi di fissare per contratto i requisiti che meglio credevano (eccezion fatta per le clausole ritenute palesemente vessatorie). Naturalmente il giurista e ogni cittadino dotato di comune buon senso è consapevole che il sinallagma tipico di ogni contratto è un'astrazione "immaginaria", una di quelle strutture inventate su cui si fonda la cooperazione sociale. In effetti il vantaggio o lo svantaggio economico generato dal contratto non può certo ridursi ai paciscienti, sempre che l'accordo possa essere anche indirettamente riscontrato. L'esempio di cui sopra lo evidenzia appieno: il consenso dello spettatore si può ritenere presunto al momento dell'ingresso nel teatro in vista dello spettacolo (non del pagamento del prezzo, supponendo che, essendo esso determinato dalle risate, venga corrisposto a fine spettacolo), ma l'analisi civilisticamente rilevante non si ferma certo qui. Infatti, il rapporto economicamente più significativo non è quello fra il potenziale spettatore e l'ente teatrale, bensì tra il primo e il proprietario dell'algoritmo che interpreta le risate. Il teatro poi, non solo determina unilateralmente le modalità del sinallagma, ma condiziona l'accesso al teatro alla cessione di dati sensibili quali i gusti talmente intimi da determinare una reazione di pancia quale la risata, a terzi. Non solo, l'utilizzo finale di questi dati (e la loro aggregazione) inconsapevolmente ceduti sotto forma di una divertente scommessa, resta nell'ombra, ma lo sono pure i veri beneficiari del "gioco" proposto dal teatro al suo utente. Per il giurista, poi, gioco e scommessa producono mere obbligazioni naturali, sicché lo spettatore uscendo potrebbe rifiutare il pagamento (salvo che abbia autorizzato l'uso della carta di credito in entrata); pertanto emerge in modo assai chiaro il ben scarso ruolo del diritto civile tradizionale che resta del tutto ineffettivo in affari di questo genere governati quasi interamente dalle capacità tecnologiche.

In effetti i contratti che concludiamo con operatori telefonici o acquistando dispositivi tecnologici pongono clausole unilaterali che, se non accettate, semplicemente impediscono l'uso del dispositivo pur in proprietà formale del titolare, (con questioni rilevanti sulla natura della proprietà)[17]. Questi contratti in realtà obbligano alla cessione forzata di dati sensibili che costituiscono la vera posta in gioco senza che il giurista abbia ancora affinati strumenti capaci di inquadrarli e soprattutto di disciplinarli visti i mutati rapporti di forza.

Per quasi quarant'anni, fino alla caduta del muro di Berlino, la Stasi, ente di sicurezza della Germania Est, ha spiato milioni di persone; apriva le lettere private e induceva coniugi e compagni a spiarsi a vicenda, violando qualunque tipo di legame fiduciario e

[16] U. Mattei - A. Quarta, *Punto di svolta. Ecologia, tecnologia e diritto privato. Dal capitale ai beni comuni,* cit.

[17] *Ibid.*.; U. Mattei, *Trattato di diritto civile, La proprietà*, Torino, 2015.

accumulando informazioni contenute in 112 chilometri lineari di documenti.
Trent'anni dopo si raccolgono più dati che mai sul nostro conto. Siamo costantemente sotto sorveglianza: quando usiamo la carta di credito per pagare, il cellulare per comunicare, il carrello per fare la spesa o la bicicletta in *sharing*.
Il giurista non può sospendere il senso critico facendosi affascinare dai piaceri (veri e propri *circenses*) che ci propone il nuovo Grande Fratello[18]. Dovremmo piuttosto concentrarci sugli innumerevoli effetti pregiudizievoli che vedevamo quando creati dalla Stasi ma che tendiamo a sottovalutare quando nascosti dalla seduttività della società dello spettacolo[19]. Pare conveniente riassumere queste criticità in tre macro-tipologie: sorveglianza a fini di marketing; sorveglianza per giudicare, punire ed eventualmente anticipare comportamenti delittuosi; effetti dei Big Data sulla privacy di ciascuno di noi, tema specifico di questo nostro studio.
Naturalmente le tre tipologie sono interconnesse perché dagli argomenti che Twitter rileva starci a cuore si possono desumere tanto elementi sulla nostra occupazione o personalità, utili a fini commerciali, quanto elementi utilizzabili dalle polizie nella repressione giustificata dalla "prevenzione del crimine". Difficile immaginare, come meglio vedremo, che in queste condizioni un assetto normativo globale della privacy basato sul "consenso" possa restituire centralità al diritto.
È noto che il settore privato non è certo l'unico a usare disinvoltamente i Big Data sfruttando il diffuso analfabetismo tecnologico che ci ha progressivamente trasformati da soggetti (cittadini) a merci (i nostri dati)[20]. Lo fanno anche i governi.
Per esempio, stando ad un'inchiesta effettuata dal Washington Post nell'ormai lontano 2010, pare che la U.S. National Security Agency (NSA) intercetti e archivi ogni giorno 1,7 miliardi di email, telefonate e altre comunicazioni tra cittadini americani e tra loro e stranieri.
Ma perché raccogliere tutti questi dati? La risposta si ricollega al modo in cui si è evoluta la sorveglianza dell'era dei Big Data. In passato gli investigatori applicavano delle pinzette ai fili del telefono per raccogliere informazioni su un sospetto, puntando a conoscere proprio quell'individuo. Oggi l'approccio è a monte diverso: siamo soliti dire che "le persone sono le loro informazioni"[21], l'aggregato delle loro relazioni sociali. Ciò significa che per studiare a fondo un individuo gli analisti devono poter accedere alla più vasta raggiera possibile di dati che lo circondano, coinvolgendo naturalmente moltissime altre persone. Una volta ciò era tecnicamente difficile e molto costoso, oggi è semplice e a costo quasi zero. Siccome poi i governi non possono sapere chi saranno i prossimi sospetti di attentati terroristici tanto vale immagazzinare più informazioni possibili per poterle estrarre all'occorrenza con una forza computazionale che aumenta esponenzialmente secondo la legge di Moore[22].
Da qui lo svilupparsi, in particolare negli stati più conservatori d'America, delle "in-

[18] G. Orwell, *1984*, Milano, 2016.

[19] G. Debord, *La società dello spettacolo,* Milano, 2002.

[20] Sul passaggio da cittadino a consumatore a merce vedi U. Mattei - A. Quarta, *Punto di svolta. Ecologia, tecnologia e diritto privato. Dal capitale ai beni comuni,* cit.

[21] L. Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality,* Oxford, 2014.

[22] J. Rifkin, *La società a costo marginale zero,* Milano, 2014.

dagini a strascico".

Tuttavia, per preoccupante che possa essere la capacità delle imprese e dei governi di mettere le mani sulle nostre informazioni personali, con l'avvento dei Big Data emerge un problema ancora più grave: l'utilizzo di previsioni per giustificare indagini mirate e per giudicarci.

La scena di apertura del film "Minority Report"[23] ritrae una società in cui le previsioni sono così accurate da consentire alla polizia di arrestare gli individui prima che commettano i delitti. Le persone vengono incarcerate non per quello che hanno fatto ma per quello che stanno per fare. Notoriamente il film attribuisce questo intervento preventivo della forza pubblica ai Precog, individui dotati di poteri extrasensoriali di precognizione grazie ai quali la polizia può punire non già la commissione del fatto in sé, bensì la mera intenzione di compierlo.

Una tale organizzazione sociale, come ovvio, scardinerebbe le basi del diritto penale quali, ad esempio, la nozione di tentativo (*conditio sino qua non* affinchè possa scattare la punibilità) *ex* art. 56 c.p; esso infatti richiede per la sua realizzazione l'estrinsecazione nel mondo reale di un intento manifestato tramite "atti idonei, diretti in modo non equivoco", non essendo punibile il mero proposito criminoso. Come autorevolmente sottolineato da V. M. Schonberger[24], se le previsioni che scaturiscono dai Big Data fossero perfette, se gli algoritmi fossero in grado di prevedere il nostro futuro con assoluta chiarezza, non avremmo più alcuna libertà di azione e ci comporteremmo esattamente secondo quanto stabiliscono le previsioni. Se potessero esistere delle previsioni perfette esse negherebbero la volizione umana ossia la condizione necessaria per tutti i reati dolosi e cioè per la stragrande maggioranza di quelli previsti dal codice penale. Paradossalmente, la perfetta prevedibilità ci priverebbe della libertà di scelta, sollevandoci così da ogni responsabilità. Queste sono le inquietanti frontiere etiche aperte dalle nuove tecnologie che sempre maggiormente ricostruiscono i nostri percorsi cognitivi in modo assolutamente (e forse pure completamente) condizionato dalle sequenze del DNA[25].

È chiaro poi che previsioni perfette sono (al momento) impossibili, come dimostrato dalle frontiere della scienza teorica e della meccanica quantistica che nel mondo dell'infinitamente piccolo si basano interamente su mere probabilità. L'analisi dei Big Data può prevedere che un certo individuo ha buone probabilità di mettere in atto un certo comportamento, ma basta che sbagli una volta per condurre un innocente in galera. Oggi la probabilità di errore è statisticamente ben più alta dell'1%. Tuttavia aumentando i dati a disposizione e la capacità computazionale, sistemi quali Blue CRUSH e FAST sono sempre più utilizzati. Il primo indica ai funzionari di polizia aree di interesse precise in termini di tempo e geolocalizzazione del luogo in cui è più probabile che avvengano omicidi o fatti di sangue ed il secondo tenta di identificare potenziali terroristi monitorandone i segni vitali come il linguaggio non verbale o altri aspetti della persona, (una sorte di pericolosa macchina della verità).

---

[23] S. Spielberg, *Minority Report,* produzione Dreamworks, 2002.

[24] V. M. Schönberger - K. Cukier, *Big Data, una rivoluzione che trasformerà il nostro modo di vivere già minaccia la nostra libertà,* Milano, 2013.

[25] U. Mattei - F. Capra, *Ecologia del diritto. Scienza, politica, beni comuni,* Sansepolcro, 2018.

Un ulteriore impiego dei Big Data si ha nell'utilizzo degli algoritmi da parte dei giudici. Tralasciando l'aspetto comune della predizione tra l'utilizzo dei grandi dati da parte delle forze dell'ordine e dei giudici, in questo secondo caso non si ha una pluralità di soggetti sotto osservazione e potenziali criminali, bensì un unico soggetto, verso il quale l'utilizzo dei Big Data non solo è ontologicamente inutile ma spesso diventa discriminatorio[26]. Ammettendo anche il paradosso secondo cui la maggior parte delle persone di colore, povere e residenti nei sobborghi cittadini, abbia una maggiore probabilità statistica di commettere reati, come si fa a decidere l'uscita su cauzione di un possibile sospetto sulla base di dati statistici relativi a soggetti a lui vicini per origine familiare o reddito percepito? La risposta a questo quesito etico ci viene fornita da uno dei numerosi algoritmi utilizzati ormai da anni nei tribunali di alcuni fra gli stati americani più conservatori. In particolare esso prevede tre tipi di risultati: l'imputato si presenterà in tribunale per le udienze, commetterà un nuovo reato e commetterà un crimine violento. Stabilisce la probabilità di questi eventi in base a nove fattori tra cui età, precedenti penali, denunce ricevute e calcola il punteggio. Il programma in questo caso non considera fattori come l'origine razziale o familiare perché ciò porterebbe direttamente a discriminazioni. Tuttavia, un' inchiesta,[27] tra le varie che si sono succedute sull'uso di questo particolare algoritmo, dimostra l'emergere di pregiudizi razziali dovuti, sempre secondo lo studio, a pregiudizi facenti capo agli stessi programmatori degli algoritmi o anche, nel caso in cui il coder sia imparziale, possono non esserlo le decisioni legate alla gestione dei dati.
Lo spazio lasciato di fatto libero dal giurista lo conquista chi è capace di controllare la tecnologia, chi ha gli strumenti per comprenderla e per forgiarla. A fronte di questo epocale cambiamento il giurista, limitato dagli attuali strumenti ed apparati valoriali, finisce per proporre norme che, nel tentativo di regolamentare l'utilizzo di Big Data ed intelligenza artificiale, si rivelano obsolete.

3. I limiti della tutela del diritto alla privacy tra validità ed (in)efficacia

Il problema senz'altro più dibattuto tra giuristi ed esperti informatici che i Big Data schiudono è quello della privacy.
A questo punto occorre un chiarimento terminologico e metodologico: quando parliamo di Big Data solitamente non intendiamo dati personali bensì dati anonimizzati o per lo meno pseudonimizzati o inferiti, ossia non riconducibili all'interessato e cioè alla persona cui i dati riguardano, oppure, nel secondo caso, dati che «non possono più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile»[28]. In realtà tutto ciò è vero in parte, in

[26] A. Garapon, *Justice Digitale: Revolution graphique et rupture anthropologique*, Paris, 2018.

[27] L'inchiesta in oggetto è disponibile sul sito investigativo *propublica.org*.

[28] Art. 4 GDPR.

quanto, se è pur vero che i Big Data non contengono informazioni personali, certamente la maggior parte dei dati che vengono generati oggigiorno e poi riutilizzati includono effettivamente informazioni di carattere personale e le aziende hanno svariati incentivi ad acquisirne di più, a conservarli più a lungo, a ricondurli al soggetto cui si riferiscono e a riutilizzarli. I dati, inoltre, potrebbero anche non configurarsi come informazioni personali, ma con i processi impiegati per il trattamento dei Big Data si possono ricondurre facilmente all'individuo a cui si riferiscono. Si pensi alla gestione delle utenze. Si stanno introducendo dei contatori elettrici "intelligenti" che raccolgono dati per tutta la giornata, con una frequenza che può arrivare a 6 secondi ed anche il modo in cui le apparecchiature elettriche richiamano energia, ossia quella che in gergo tecnico viene chiamata "firma di prelievo" specifica ci dice molto delle abitudini di una famiglia: uno scaldabagno richiederà una quantità di energia diversa da quella di un pc o ancora di una lampada utilizzata per coltivare piantine di marjuana. L'uso domestico dell'energia elettrica rivela certamente informazioni confidenziali.

Ma qui l'interrogativo che vogliamo porci non è tanto se i Big Data accrescono il rischio per la privacy (ciò è pacifico), ma se vengono a modificare la natura del rischio e di conseguenza le soluzioni[29].

Come dovrebbe emergere dal precedente paragrafo, uno dei tanti diritti, e forse il più di tutti, interessati dall'uso massivo delle nuove tecnologie è certamente il diritto alla privacy, declinato nelle sue due accezioni di (1) diritto alla riservatezza e (2) diritto alla protezione dei dati personali. Come noto tale distinzione viene evidenziata dalla Carta dei diritti fondamentali dell'Unione europea, che gli dedica due articoli separati, rispettivamente l'art. 7 rubricato "rispetto della vita privata e della vita familiare" e l'art. 8 dal titolo: "protezione dei dati di carattere personale" [30].

Naturalmente i due diritti sono intrinsecamente connessi[31]. La legislazione europea (e nazionale) succedutasi negli anni è corposa e certamente più garantista se confrontata, per esempio, con quella statunitense[32]; ciò nonostante l'aspirazione protettiva, se fondata su strutture giuridiche inadeguate, difficilmente può considerarsi misura del successo.

Il bisogno di armonizzazione delle leggi sulla privacy dei vari stati europei ha condotto all'approvazione, nel maggio 2016, del regolamento (UE) 2016/679 denominato in breve Regolamento Generale sulla protezione dei dati personali ed entrato in vigore il 25 maggio 2018.

Il regolamento, direttamente applicabile in tutti gli stati membri, estende il suo ambito normativo anche alle imprese situate fuori dai confini dell'Unione che offrano servizi o prodotti alle persone fisiche che si trovino sul suo territorio. Ciò per la prima volta ed allo scopo di evitare che vengano facilmente eluse le più stringenti leggi privacy

[29] V. Zeno Zencovich - G. Codiglione, *Ten Legal Perspectives on the "Big Data Revolution"*, in *Concorrenza e mercato,* 23, 2017, 39 ss.

[30] Si veda a proposito: S. Rodotà, *Vivere la democrazia,* Bari-Roma, 2018; Id., *Il diritto di avere diritti,* Bari-Roma, 2013; Id., *Il mondo nella rete. Quali i diritti, quali i vincoli,* Bari-Roma, 2014.

[31] S. Rodotà, in P. Conti (a cura di), *Intervista su privacy e libertà*, 2005; S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione,* Bari-Roma, 2004.

[32] C. Focarelli, *La Privacy. Proteggere i dati personali oggi,* Bologna, 2015; G. D'Acquisto - M. Naldi, *Big Data e privacy by design,* Torino, 2017.

europee semplicemente spostando lo stabilimento all'estero. Questo è uno dei tanti criteri scelti dal legislatore per rendere effettivo il rispetto dei parametri europei, cercando di ovviare allo strutturale vantaggio della *corporation* transnazionale rispetto agli stati di cui si è detto in apertura.

Il secondo elemento motivato dalla ricerca dell'effettività è costituito dai principi della *privacy by design* e *privacy by default* sanciti espressamente dall'art. 25, par. 1, GDPR, rubricato: "Protezione dei dati dalla progettazione e protezione per impostazione predefinita". Esso chiarisce cosa significa tale principio in questi termini «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati».

Inoltre, esplicitando il principio della *privacy by default* dispone: «Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento».

Nell'enunciare questi due principi ed in altre disposizioni regolamentari nonché nei considerando, il legislatore europeo si dimostra invero piuttosto attento nella previsione di tutele che siano effettive anche quando premette «tenendo conto dello stato dell'arte e dei costi di attuazione» evitando pertanto di porre norme che, per la difficoltà di attuazione o per l'impossibilità dei mezzi finanziari, finiscano col rimanere sulla carta.

Tuttavia col fissare il requisito della *privacy by design* in capo ai soggetti che trattano i dati, il nuovo regolamento devolve, di fatto, la parte regolamentare a monte del trattamento ai programmatori di sistemi informatici che, creando software "a prova di privacy", si sostituiscono ai giuristi nella posa in opera del sistema regolamentare. Sono cioè nuovi soggetti, privi di sapienza giuridica, a dare legittimità alla pratica effettiva validandone le norme. L'algoritmo diviene così fonte sostanziale del diritto e l'ingegnere informatico si surroga al giurista come detentore della potestà legislativa occulta[33].

Non è questa la sede per soffermarsi in dettaglio sulla nuova legislazione perché intendiamo offrire qui un semplice catalogo problematico da cui risulti come l'effettività, intesa soprattutto come efficacia ma anche come validità della norma di diritto positivo venga sfidata dai nuovi assetti.

Una delle critiche più aspre mosse al legislatore europeo[34] è stata quello di incentrare, ancora una volta, il trattamento dei dati sulla base giuridica del consenso, che sebbene sulla carta funga da criterio residuale, nella realtà viene usato, a parere di chi scrive, troppo frequentemente. Già la direttiva 96/45/CE infatti prevedeva il consenso quale

[33] A. Gambaro, *Il successo del giurista,* in *Il Foro Italiano*, 106(3), 1983, 85 ss.

[34] Sul punto si v. F. Pizzetti, *Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 46/95 al nuovo Regolamento europeo,* Torino, 2016.

perno per ogni trattamento di dati personali, anche sensibili ed effettuati su larga scala. Lo stesso viene ripreso dal regolamento che, sulla scorta delle definizioni mutuate dalla vecchia direttiva, stabilisce all'art. 4, par. 11, che esso dev'essere liberamente prestato, specifico, informato ed inequivocabile, nonché suscettibile di essere provato da parte del titolare del trattamento (*ex* art. 7, par. 1).

Questa tralatizia impostazione si mostra insipiente, o comunque non desiderosa di intervenire sulle autentiche trasformazioni strutturali prodotte dai Big Data e dall'evoluzione tecnologica ormai capace di impattare anche i dati sensibili, si pensi ai biometrici o ai genetici.

Il requisito di specificità che richiede che il consenso sia prestato per ogni singolo trattamento ed il fatto che esso debba essere informato, ossia l'interessato ne debba sapere l'uso attuale e tutti gli usi futuri, si liquefanno davanti ad imprese e aziende che trattato dati eterogenei raccolti in modo eterogeneo, conservati e poi riutilizzati per trattamenti futuri non previsti né prevedibili necessariamente al momento della raccolta.

Il legislatore europeo, poi, per evitare di cadere nella facile critica delle difficoltà tecniche di richiedere un consenso fondato su siffatti requisiti, all'art. 6 sulla liceità del trattamento elenca una serie di requisiti di cui almeno uno necessario per rendere lecito il trattamento dei dati personali.

Tali requisiti quali la presenza di un obbligo di legge, l'esecuzione di un contratto, un interesse legittimo e via discorrendo rendono il principio cardine del consenso informato, già di per sé debolissimo, residuale e necessario solo qualora non sussista uno degli altri requisiti.

Il consenso, legato com'è a una concezione datata dell'individualismo proprietario, pone problemi anche avuto riguardo agli *small data* e soprattutto a quei dati che la nuova norma definisce all'art. 9 come categorie particolari di dati personali, nella cui definizione rientrano i dati sensibili ossia «dati personali che rivelino l'origine raziali o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati generici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona». In linea di principio vi è un divieto di trattare tali dati salvo quando sussistono anche uno solo dei requisiti sanciti al par. 2 di cui il primo è appunto il consenso esplicito dell'interessato.

Vi è poi una seconda categoria di dati il cui trattamento è legittimo solo in presenza di determinati requisiti che sono i dati giudiziari, in particolare relativi a condanne penali e reati *ex* art. 10 del regolamento, per i quali, ovviamente, il consenso dell'interessato non funge da requisito necessario al trattamento.

Come se non bastasse, il 28 novembre 2018 è stato pubblicato sulla Gazzetta ufficiale dell'Unione Europea un secondo regolamento, da affiancare al GDPR, denominato "Regolamento sul libero flusso dei dati non personali". Tale fonte legislativa è naturalmente indirizzata alle imprese e multinazionali che intendono trattare dati per scopi che vanno dal marketing alla pubblicità e solo indirettamente riguarda i soggetti privati. La finalità, dice la Commissione[35], è di incentivare la creazione di un'economia dei dati europea e l'utilizzo da parte delle imprese del *cloud computing*, strumento dalle immense

[35] Il documento è titolato: *Un quadro per il libero flusso dei dati non personali in Europa,* in *ec.europa.eu*, 19

capacità di archiviazione, condivisione e riutilizzo di dati.
In realtà è noto tra gli addetti ai lavori che la motivazione è in larga misura, ancorché occultamente, poliziesca. La creazione di luoghi di archiviazione localizzati in territorio europeo rende le imprese titolari dei dati libere di delocalizzare la tenuta dei propri dati anche in altri stati europei (fino ad ora infatti le autorità pubbliche italiane erano costrette ad archiviare dati solo sul territorio italiano) agevolando così la cooperazione internazionale nella prevenzione del crimine e soprattutto del *cybercrime*. I fornitori dei servizi *cloud* o simili saranno infatti sempre tenuti, sulla base dell'art. 5 del summenzionato regolamento a comunicare alle autorità di polizia statali, qualora richiesti, i dati archiviati nei loro sistemi rendendone così più agevole il reperimento e quindi la conseguente cattura del colpevole[36].

4. Una risposta giuridica alla sfida dei Big Data: la privacy come *common* digitale

Nell'epoca odierna le ICT detengono e consentono l'esercizio di un enorme potere computazionale producendo enormi quantità di dati tanto da indurci a parlare di età dello zettabyte[37]. Tali dati vengono prodotti da tutti gli utenti della rete in modo tendenzialmente aperto e dunque "democratico", ma non altrettanto apertamente e democraticamente vengono utilizzati, come abbiamo avuto modo di vedere. Come per magia, le impronte individuali che ciascuno di noi lascia indelebili in rete, proprio come quelle di Neil Armstrong immutabili sulla luna dal 1969, vengono aggregate e divengono entità collettive, in cui il valore dell'aggregato trascende di gran lunga quello delle parti che lo compongono. Questi collettivi, che rendono sempre più semplice discendere alle sue parti, determinandone financo i comportamenti, prevedibili in modo statistico, proprio come nel mondo dell'infinitamente piccolo, non sono governabili con gli strumenti tradizionali del diritto, quelli che hanno prodotto, a seguito di una evoluzione storica lunga come la modernità, le condizioni del costituzionalismo liberale in cui ancora ci illudiamo di vivere.
Nella fase attuale il capitalismo è cognitivo[38] e la Rete non solo ne crea le condizioni tecnologiche, ma costituisce lo spazio in cui si condividono idee, opinioni e lotte politiche. Sappiamo come la capacità tecnologica di utilizzare internet, i social ed i Big Data costituisca una forza poderosa nel raggiungere e financo determinare le preferenze dell'elettorato attivo o spolverare di democraticità la selezione di quello passivo (si pensi alla dibattuta piattaforma Rousseau del M5S).
I collettivi si formano in rete con assoluta semplicità (si pensi al Movimento delle Sardine nato nell'autunno dell'anno passato durante la campagna elettorale per le elezioni regionali in Emilia Romagna), riunendo persone con caratteristiche, idee politiche o problemi comuni, o semplicemente perché abitanti in luoghi finitimi; si pensi alla cre-

settembre 2017.

[36] Si veda nota 23.

[37] L. Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality,* cit.

[38] U. Mattei, *Beni comuni, un manifesto,* cit.

azione delle chat di gruppo create successivamente all'ideazione delle piattaforme di messaggistica istantanea quali per esempio WhatsApp Messenger. Ovviamente si tratta di aggregati estremamente fluidi ma molto significativi per chi detenga il controllo di algoritmi capaci di elaborarli in tempo reale. Le grandi aziende tecnologiche che raccolgono queste miriadi di dati sono in grado di porre in essere azioni di "micro-management" delle nostre soggettività trasformando l'informazione in suggestione[39] o confinandoci in quelle che in gergo informatico sono dette *filter bubbles* o se si preferisce bolle di filtraggio. Ha fatto un certo scalpore a questo proposito il caso Cambridge Analityca.

L'obiettivo non è chiaro all'utente consumatore e non è nemmeno detto che ci sia un fine diverso dal semplice connettere persone al fine di estrarre il valore economico della cooperazione, il che costituisce la vocazione strutturale della *corporation*.

Il noto filosofo dell'Università di Oxford, Luciano Floridi, da tempo quando ci parla della potenzialità dei Big Data afferma che nel mondo caratterizzato dall'eccesso di informazione (*over-information),* l'interesse delle multinazionali ma anche dei governi non è più legato al *targeting,* ossia alla profilazione del singolo individuo, perché ciò sarebbe troppo complicato e poco redditizio. Oggi la strategia è il *group-targeting,* ossia dividere le persone in gruppi sulla base di comuni preferenze dimostrate o scelte effettuate. Il gruppo non solo politicamente ma anche economicamente è più forte dell'individuo e sono soltanto i giuristi, oggi ancor prigionieri dell'ideologia umanistica dominante la modernità, ad insistere sulla tutela giuridica dell'individuo e così facendo spuntando le armi con cui il "giuridico" cerca di governare i processi trasformativi del presente. Di qui la drammatica crisi dell'effettività giuridica formalmente legittimata, da cui ha preso le mosse il presente scritto.

Se la fattualità è collettiva, la ricerca della legittimità è ancora di segno opposto (si pensi al consenso informato dell'individuo), con tutte le criticità che in questo scritto abbiamo cercato di evidenziare. Da un lato la personalità di ciascuno di noi assume rilevanza se inserita in un gruppo, dall'altra però il legislatore europeo e nazionale continuano a definire la privacy come diritto soggettivo azionabile in giudizio individualmente. Tale discrasia non è solo linguistica ma si ripercuote sul diritto medesimo in quanto sempre più di frequente violando la privacy individuale si sconfina anche in quella altrui, mostrando drammaticamente l'insufficienza del modello monadico. Violando per esempio l'art. 7 della Carta dei diritti fondamentale dell'Unione Europea, si invade contestualmente anche la sfera privata delle persone che vivono con il soggetto leso e quanto ai vincoli di parentela, l'esempio più paradigmatico sono i dati genetici. Il GDPR definisce i dati genetici come: «i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia». Le caratteristiche genetiche pongono non pochi problemi in termini di tutela dei dati personali. Essi rientrano nella tipologia dei dati particolari, ossia sensibili e pertanto il loro trattamento è in linea di principio vietato come sancito dall'art. 9, par. 1, salvo che sussista uno degli elementi elencati nel par. 2. In ogni caso mostrano come il modello del consenso informato sia assolutamente inadatto proprio dal punto di vista strutturale.

[39] J. Lanier, *Dieci ragioni per cancellare subito i tuoi account social*, Milano, 2018.

A ben vedere infatti anche in mancanza di violazione della privacy, ossia a seguito di consenso informato effettivamente rilasciato da un individuo, quest' ultimo coinvolge necessariamente anche posizioni altrui con le quali nella realtà fattuale è intrinsecamente connesso. Né si tratta solo di cerchie strette di parenti. Recentemente un gruppo di studiosi ha pubblicato sulla rivista Science uno studio che dimostra come le informazioni genetiche anonime concesse dai milioni di americani che si sono fatti attrarre dalla prospettiva di conoscere meglio i propri geni accettando offerte di test gratuiti, combinate con Big Data di contesto e un semplice esemplare di DNA (un capello reperito in un certo luogo), possano portare all'individuazione probabilistica estremamente precisa del titolare di questo, anche se quest'ultimo non ha mai fatto il test![40]
Andrebbe ben oltre la portata di questo scritto che, come detto, non vuole essere più che una rassegna problematica, offrire le linee di una *pars construens* di una visione della privacy autenticamente consapevole della struttura relazionale profonda della nostra stessa identità. La natura obsoleta di ogni epistemologia meccanicistica che immagina la società come esito della somma algebrica di monadi individuali è stata oggi largamente denunciata anche nel diritto[41]. Noi siamo relazione e i social media hanno reso questo dato evidentissimo. Consentendo al trattamento dei miei dati personali coinvolgo necessariamente anche in miei "amici", che questi siano o meno titolari di un account. Per pensare alla privacy (come a molte altre istituzioni giuridiche) in modo strutturalmente adeguato al mondo che si sposta sempre più alla sua frontiera virtuale, occorre un giurista capace di padroneggiare il pensiero sistemico[42] ed una visione profondamente relazionale e collettiva dell'esperienza sociale di cui il diritto non può farsi carico se resta prigioniero del suo individualismo ottocentesco. Una privacy 4.0 si può sviluppare soltanto recuperando effettività ad un diritto a sua volta profondamente trasformato dalla tecnologia. Ciò richiede una riflessione seria sul comune come istituzione collettiva capace di restituire resilienza nei confronti della concentrazione del potere globale[43]. Solo il giurista capace di imbarcarsi in questa impresa non abdica al proprio ruolo e non diviene sostituibile dal *coder* e dall' algoritmo. I primi studi sulla privacy come accesso sembrano muovere qualche (timido) passo in questa direzione.

[40] Science, *Millions of Americans Could Be Identified Using Genetic Databases, even if they have never taken a DNA test,* 14 ottobre 2018.

[41] Vedi U. Mattei - F. Capra, *Ecologia del diritto. Scienza, politica, beni comuni*, cit.

[42] F. Capra - P.L. Luisi, *Vita e natura. Una visione sistemica,* Sansepolcro, 2017.

[43] A. Quarta - M. Spanò, *Beni comuni 2.0. Contro-egemonia e nuove istituzioni,* Milano, 2016.