Privacy e informazione nell'era dei Big Data

Arianna Maceratini

Abstract

L'informazione costituisce, attualmente, una delle principali risorse economiche del processo produttivo e, di conseguenza, le attività di raccolta, selezione e monitoraggio dei dati personali assumono una fondamentale rilevanza poichè rivolte alla capillare targettizzazione e fidelizzazione del consumatore. In questa direzione, la privacy, da tutela individualistica del diritto ad essere lasciati soli, assume il significato di diritto al pieno controllo delle informazioni personali. L'analisi dei Big Data si spinge sino alla ricerca e all'esame di ogni possibile correlazione tra i dati e gli algoritmi impiegati nei processi decisionali. Se l'uso cooperativo e partecipato nella sfera pubblica di alcune tipologie di Big Data può rivestire un sicuro interesse sociale, in altri casi l'utilizzo di tali conoscenze solleva notevoli criticità concernenti la tutela dei dati personali, il loro sfruttamento economico, la presenza di un'effettiva consapevolezza e libertà nella manifestazione del consenso al loro trattamento. Ulteriori incognite, conseguite all'impiego dei Big Data, sono rappresentate dalla polarizzazione dell'informazione in capo a pochi intermediari digitali che palesa tutta l'asimmetria tra chi offre il servizio informativo e il suo fruitore, aggravata dall'intrasparenza e dalla selettività dei criteri posti alla base del funzionamento dell'algoritmo, problematiche che si riflettono sulla piena esplicazione dei diritti di libertà e sul futuro della democrazia. Si mostra, allora, tutta l'urgenza di un'efficace regolazione dei Big Data e, più in generale, delle informazioni personali circolanti online, *ispirata ai valori costituzionalmente garantiti e diretta alla tutela dell'individuo dall'impiego improprio delle tecnologie informatiche, nella prospettiva di un'innovativa delineazione di modelli di cittadinanza digitale attiva, a fondamento di un'effettiva libertà di costruzione personale.*

Information is currently one of the main economic resources of the production process and, consequently, the collection, selection and monitoring of personal data assume a fundamental importance as they are aimed at capillary consumer targeting and retention. In this direction, privacy, from individualistic protection of the right to be left alone, takes on the meaning of the right to full control of personal information. The Big Data analysis goes as far as searching and examining any possible correlation between the data and the algorithms used in the decision-making processes. If the cooperative and participatory use in the public sphere of some types of Big Data can be of certain social interest, in other cases the use of such knowledge raises significant critical issues concerning the protection of personal data, their economic exploitation, the presence of an effective awareness and freedom in the manifestation of consent to their treatment. Further unknowns, resulting from the use of Big Data, are represented by the polarization of information by a few digital intermediaries that reveals all the asymmetry between those who offer the information service and its user, aggravated by the transparency and the selectivity of the criteria places at the base of the functioning of the algorithm, problems that are reflected on the full explanation of the rights of freedom and on the future of democracy. All the urgency of an effective regulation of Big Data and, more generally, of personal information circulating online, inspired by the constitutionally guaranteed values and directed to the protection of the individual from the improper use of information technology, is shown in the the prospect of an innovative delineation of models of active digital citizenship which are the foundation of an effective freedom of personal construction.

Parole chiave

Informazione; Dati Personali; Privacy; Consenso; *Internet Of Things; Big Data;* Polarizzazione; Algoritmi; Democrazia.

Keywords

Information; Personal Data; Privacy; Consent; Internet Of Things; Big Data; Polarization; Algorithms; Democracy.

Introduzione

"Siamo entrati nell'era che viene chiamata post-moderna, ed è caratterizzata dall'enorme progresso, vertiginoso ed irreversibile della trasformazione tecnologica e conseguentemente anche tecnocratica del mondo. Dal giorno in cui Bacone disse che la scienza è potere, l'uomo ne ha percorsa di strada!"[1] Così, nei primi anni Novanta, scriveva Bobbio ne *L'età dei diritti* mostrando come i diritti definiti di nuova generazione[2] nascano, fondamentalmente, dallo sviluppo tecnologico e dai possibili riflessi di quest'ultimo sul diritto alla vita, alla libertà, alla sicurezza personale[3]. In nessun caso si potrebbe, infatti, concepire un'indifferenza del tradizionale quadro dei diritti all'odierno contesto, caratterizzato dall'irrefrenabile progresso delle tecnologie informatiche, tale da sbiadire, sino a rendere irrilevante, la tradizionale contrapposizione tra vecchi e nuovi diritti[4] mettendo, così, in luce tutta la capacità del diritto di aderire ai mutamenti di una società complessa e in movimento[5].

In questo lavoro, riferendoci principalmente ai Big Data, si vedrà come la possibilità di raccogliere, elaborare ed incrociare le informazioni personali abbia condotto ad una ridefinizione della sfera privata e, prima di tutto, dell'autodeterminazione individuale, capace di mettere al centro dell'attenzione e della riflessione la conoscenza e l'effettività della sua garanzia.

1 N. Bobbio, *L'età dei diritti*, Torino, 1990, p. 263.

2 Cfr. *ibidem*.

3 Cfr. *ibidem*.

4 Cfr. S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2012, p. 69.

5 Cfr. C. Faralli, *Introduzione*, in: A. Ballarini (a cura di), *Novecento del diritto*, Torino, 2019, p. 5.

La Società dell'informazione e il diritto alla privacy

L'informazione costituisce, nella cosiddetta *new economy*, una delle principali risorse economiche del processo produttivo e la capacità di controllare e vendere conoscenza rappresenta una sofisticata e redditizia forma di scambio commerciale, laddove il maggior profitto proviene non tanto dai tradizionali processi produttivi e prodotti, quanto dal controllo delle informazioni e delle tendenze di mercato che permettono di ottimizzare il rapporto tra fornitore e utente, in direzione della fidelizzazione di quest'ultimo[6]. Di fondamentale rilievo appaiono, dunque, la raccolta, la selezione significativa delle informazioni e il loro monitoraggio, mirati ad una targettizzazione sempre più capillare, capace di individuare e tratteggiare le caratteristiche del singolo consumatore. La delineazione di profili e preferenze individuali, a sua volta, contribuisce ad influenzare il comportamento soggettivo come dimostrano, in modo estremamente significativo, i fenomeni dell'*anticipatory shipping* e dell'*anticipatory selling*, sviluppati da Amazon, capaci di anticipare e di indurre, apparentemente senza alcuna forzatura, i futuri acquisti della clientela[7]. "L'efficienza della rivoluzione digitale si manifesta anche nelle 'raccomandazioni', nei 'suggerimenti' algoritmici che riceviamo dalle pubblicità dei motori di ricerca o evidenziate nei siti di *e-commerce*: occasioni che *potrebbero* interessare, come hanno interessato

6 Cfr. ad es. J. Rifkin, *The Age of Access: The new Culture of Hypercapitalism, Where All of Life is a Paid-for-Experience*, New York, 2000, trad. it., *L'era dell'accesso*, Milano, 2001, p. 65.

7 Al riguardo, cfr. D. Talia, *La società calcolabile e i big data. Algoritmi e persone nel mondo digitale*, Catanzaro, 2018, p. 25.

altri, simili a noi, prima di noi"[8]. Il tradizionale dibattito sulla privacy – che dalla tutela della riservatezza individuale muove, in modo sempre più accentuato, verso la garanzia ed il controllo delle proprie informazioni - si fa, allora, acceso quando si parla di monetizzazione dei dati, cioè quando è la stessa privacy che diviene risorsa economica e quando sono gli utenti a cederla in cambio di servizi gratuiti[9], essendo evidente come le informazioni di natura personale siano intimamente connesse ai diritti della persona e ponendo, dunque, il loro sfruttamento economico pressanti interrogativi di ordine etico e giuridico, coinvolgendo la tutela di diritti fondamentali[10].

Il concetto di privacy, nella duplice accezione di garanzia della sfera più riservata dell'essere umano e di tutela dei dati personali che lo riguardano, ha subito considerevoli evoluzioni nel tempo e nello spazio. Potendo qui solo brevemente accennare a tale percorso, va ricordato come già nell'antichità più remota l'uomo cercasse momenti di solitudine al fine di proteggere la vita privata ed avesse sviluppato il concetto di confidenzialità e di segretezza delle informazioni. Le moderne origini del concetto di privacy si fanno, in ogni caso, risalire a due giuristi statunitensi, Samuel Warren e Luis Brandeis che, nel volume 1890-91 dell'*Harward Law Review*, diedero alle stampe il saggio *The Right of Privacy*. In tale lavoro - scaturito dalla controversia contro il periodico *Evening Gazette*, accusato da Warren di indebita ingerenza nella vita intima della consorte – i due autori si interrogavano, appunto, su quali informazioni della vita privata dovessero rimanere segrete e quali, diversamente, potessero divenire di pubblico dominio, delineando, così, il diritto alla privacy attraverso il valore intrinseco che esso possiede per il suo titolare. La nozione di privacy si è poi estesa fino a parlare, attualmente, di *computer privacy*, ad indicare la necessità di avere il controllo del flusso di informazioni personali, circolanti attraverso gli elaboratori elettronici e la rete telematica, dati che, se correttamente interpretati, sono in grado di rivelare i più riservati dettagli dell'esistenza umana[11]. In Italia, la disciplina relativa alla protezione dei dati personali è contenuta nel d.lgs. 30 giugno 2003, n. 196, denominato "Codice in materia di protezione dei dati personali" (Codice Privacy), provvedimento volto a ricondurre ad unità le innumerevoli disposizioni del settore succedutesi negli anni e ad introdurre le più significative innovazioni dell'Autorità Garante e delle Direttive europee in materia di riservatezza delle comunicazioni elettroniche. Tra queste ultime, occorre menzionare la Direttiva UE n.95/46, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, avente lo scopo di armonizzare le norme in materia di protezione dei dati personali, di garantire un libero flusso dei dati e di promuovere un elevato livello di tutela dei diritti fondamentali dei cittadini europei. Tale provvedimento è stato, com'è noto, recentemente abrogato dal *General Data Protection Regulation* (GDPR: Regolamento UE n. 2016/679) volto a rafforzare la riservatezza delle informazioni private implementando il sistema delle responsabilità e delle misure di sicurezza a protezione delle informazioni[12]. L'attuale significato assunto dalla privacy, da tutela individualistica e sostanzialmente passiva del diritto ad essere lasciati soli a diritto al pieno controllo delle informazioni che ci riguardino[13], è sancito, inoltre, dalla Carta dei Diritti Fondamentali dell'Unione Europea (Carta di Nizza del 2000, che all'art. 8 dispone il diritto alla protezione dei dati personali), nonchè dalla Dichiarazione dei diritti di Internet del nostro Paese - resa pubblica il 13 ottobre del 2015 durante una conferenza inter-

8 M. Delmastro, A. Nicita, *Big data. Come stanno cambiando il nostro mondo*, Bologna, 2019, p. 13.

9 Cfr. S. Palanza, *Internet of things, big data e privacy: la triade del futuro*, in" IAI, Documenti Istituto Affari Internazionali", 2016, p. 9.

10 Sull'imprescindibile nesso tra trattamento dei Big data e protezione dei diritti umani, si veda F. A. Schreiber, L. Tanca, *Etica e big data, sette principi per proteggere i diritti umani*, in: https://www.agendadigitale.eu.

11 Cfr. G. Pascuzzi, *Il diritto dell'era digitale*, Bologna, 2016, p. 48. Per un esame dell'evoluzione del concetto di privacy, cfr. ivi, pp. 43-53.

12 Il d.lgs. n. 101 del 10 agosto 2018 ha adeguato il Codice Privacy alle disposizioni del GDPR (Regolamento UE 2016 n. 679).

13 Cfr. S. Rodotà, *Il mondo nella rete*, cit., p. 31.

nazionale tenutasi presso la Sala della Regina di Palazzo Montecitorio - testo fondamentale nel garantire a ciascun individuo l'esercizio di una cittadinanza digitale attiva, nel pieno rispetto e valorizzazione della libertà, della dignità e della diversità di ogni persona, elementi fondamentali di una società della dignità, dell'uguaglianza, della libertà e della partecipazione[14].

I *Big Data*

Nella società dell'informazione, centrale è l'idea della condivisione dei dati, rinvenibili ovunque vi sia un dispositivo di memoria degli stessi[15]: questi, se analizzati singolarmente possono non risultare particolarmente significativi, ma, se esaminati con le opportune tecnologie informatiche ed in grandi volumi, possono condurre alla delineazione di modelli e di tendenze, in grado di produrre propriamente conoscenza. In questo senso, è evidente come la pervasività delle tecnologie informatiche, principalmente, come si vedrà in seguito, dell'*Internet of Things*, abbia aumentato e facilitato pratiche di sorveglianza digitale, rendendo chiunque utilizzi un dispositivo informatico connesso in rete, facilmente rintracciabile e monitorabile. Tale fenomeno è incrementato dalla circostanza che, di frequente, vede l'utente sottoscrivere un unico contratto con il medesimo fornitore di servizi - Internet, telefono, televisore - trasferendo nelle mani di un solo soggetto ingenti quantità di informazioni[16]. Sin da tali cenni, si può ben comprendere come il termine "dati personali" vada attualmente inteso in chiave evolutiva, cioè - seguendo la direzione indicata dalle linee guida Ocse del 2013 - considerando come informazioni riservate anche tutte quelle notizie personali che, se connesse ad altri dati sul medesimo individuo, possono produrre degli effetti sullo stesso; analogamente, il concetto di privacy andrebbe esteso alle informazioni che, seppur fuoriuscite dalla sfera della signoria soggettiva, contribuiscano ad identificarlo[17]: a stretto rigore, dunque, "nemmeno sui dati che sono pubblicati in Rete per una specifica finalità l'utente intende rinunciare all'aspettativa di privacy"[18]. Infatti, nell'analisi dei dati personali, si può osservare come, paradossalmente, le predizioni appaiano molto più esaustive e significative delle informazioni rilasciate consapevolmente dagli utenti[19]. In altre parole, "i modelli di *big data analytics* permettono di 'ricostruire' dati personali, indipendentemente dal loro originario rilascio, rendendo del tutto superata la tradizionale classificazione tra dati personali e dati non personali"[20]. Di conseguenza, come si è visto, un'appropriata considerazione dell'evoluzione tecnologica sembra condurre ad un'interpretazione estensiva ed in mutamento del concetto di dato personale, includendovi anche le informazioni prodotte mediante gli oggetti "intelligenti" [21].

Secondo la citata definizione OCSE, sono Big Data tutti i contenuti generati dagli utenti in Rete, inclusi *blog*, foto, video, dati comportamentali, dati sociali, dati di geolocalizzazione, dati demografici e dati identificativi in generale: contenuti che consentono l'identificazione individuale o che forniscono informazioni sugli schemi tipizzati del comportamento in-

14 Cfr. S. Rodotà, *Discorso conclusivo della Ventiseiesima Conferenza Internazionale sulla protezione dei dati (Breslavia, 13-16 settembre 2004)*

15 Cfr. D. Talia, *op. cit.*, p. 39.

16 Cfr. S. Palanza, *op. cit.*, p. 3. Una possibile soluzione, prospettata per superare il problema, è stata individuata nella limitazione del numero massimo di variabili da utilizzare nell'analisi dei Big Data, ma resterebbe aperto, anche in questa ipotesi, il problema dei dati estratti in maniera non prevista nonché delle ulteriori informazioni ottenute grazie all'efficacia predittiva degli algoritmi utilizzati, cfr. F. Casi, *Big Data ed etica dei dati*, in: www.consultadibioetica.org, p. 2.

17 Cfr. M. Orefice, *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, Canterano, 2018, p. 100.

18 Ivi, p. 105.

19 Cfr. M. Delmastro, A. Nicita, *op. cit.*, p. 36.

20 *Ibidem*.

21 Cfr. S. Palanza, *op. cit.*, p. 8. E' da notare come l'art. 1 lett. C della proposta di Regolamento sulla Privacy nelle Comunicazioni Elettroniche (*ePrivacy Regulation*) includa nella categoria dei metadati tutti i dati diversi dal contenuto, ma solo quelli trattati sulla rete e non anche i dati processati sui *devices*, come rileva anche l'Opinion del Garante Privacy Europeo del 6/2017.

dividuale[22]. I Big Data possono essere definiti anche mediante le cosiddette 4V, ovvero, *volume*, in quanto presenti in grandi quantità; *varietà*, poiché provenienti da fonti eterogenee; *velocità*, poiché i dati sono analizzati tramite sofisticati algoritmi che conducono ad una decisione in tempo reale[23]; *valore* assunto, in tal modo, dai dati[24]. Va rilevato come la maggior parte di questi dati risulti, solitamente, non strutturata, in quanto acquisita e memorizzata secondo criteri differenti da quelli che sovraintendono l'organizzazione dei tradizionali archivi elettronici[25]. In altri termini, la peculiarità e la potenzialità dei Big Data, capaci di comportare un vero e proprio cambio di paradigma nell'analisi delle informazioni[26], si rinvengono nel loro non essere stati estrapolati da campioni rappresentativi della popolazione mediante processi complessi e costosi[27], ma direttamente dall'insieme della popolazione osservata, cosicché, in termini di efficacia predittiva, nello sfruttare ogni possibile correlazione, la loro quantità prevale sull'esattezza del procedimento di analisi[28]. Nell'utilizzo dei Big Data, "l'aspirazione e l'esigenza all'esattezza vengono depotenziate. Infatti la presenza di meno errori, giocoforza, nel campionamento, consente di accettare qualche imprecisione nel computo"[29]; ciò permette di superare il tradizionale metodo di analisi dei dati, impostato sulla ricerca di relazioni causali, per giungere all'esame di ogni possibile correlazione. "Con i Big Data è solamente possibile ricercare e scoprire, individuare e analizzare andamenti e correlazioni. In moltissime attività non è necessario conoscere sempre la causa di un fenomeno, ma è più che sufficiente individuare come esso agisca e interagisca con altri e che correlazioni si stabiliscano tra loro"[30]. Viene, così, descritta un'analisi esplorativa e basata sull'inferenza, nella quale la macchina "impara direttamente" dai dati[31] e dove rilevante è il processo di lavorazione e di aggregazione delle informazioni con gli algoritmi impiegati nel processo, finalizzato al raggiungimento di una "decisione". In tal modo, i Big Data implementano l'utilizzo dell'algoritmo mentre, a sua volta, l'uso dell'algoritmo genera nuovi dati, e così via[32]. Va, inoltre, rilevato come l'analisi dei Big Data venga spesso affiancata dall'esame degli Small Data, ovvero, delle informazioni non generate dalla correlazione dei dati, ma rilevate dall'osservazione del comportamento degli utenti e delle loro *routines*, inserite nel contesto abituale di azione[33]; altrettanto significativo appare lo studio dei metadati, cioè, di quelle informazioni che sono associate ad una pagina *Web*, o ad una parte di essa, rappresentandone in modo strutturato il contenuto e il contesto di riferimento[34]. Il dato, dunque, quale descrizione di fatti potenzialmente riproducibili[35], diventa vera e propria informazione quando viene estratto, elaborato e utilizzato a fini specifici[36]. In questa direzione, si può ben comprendere come il corretto uso dei Big Data rappresenti un fattore critico per le imprese, nel costante perfezionamento e personalizzazione dei servizi offerti all'utenti: enormi quantità di dati, se non interpretati e utilizzati efficacemente, rischiano di essere altrettanto

22 Cfr. M. Delmastro, A. Nicita, *op. cit.*, p. 35.

23 Per una definizione dell'algoritmo, delle sue caratteristiche e proprietà, si veda A. C. Amato Mangiameli, *Informatica Giuridica. Appunti e materiali ad uso di lezioni*, Torino, 2015, pp. 132-34.

24 Cfr. M. Delmastro, A. Nicita, *op. cit.*, pp. 25-29.

25 Cfr. ivi, p. 10.

26 Cfr. A. Simoncini, S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in: "Rivista di filosofia del diritto", VIII (2019), n. 1, p. 92.

27 Cfr. A. C. Amato Mangiameli, *Algoritmi e big data. Dalla carta sulla robotica*, in: "Rivista di filosofia del diritto", VIII (2019), n. 1, p. 112.

28 Cfr. M. Orefice, *op. cit.*, pp. 149 sgg.

29 F. Casi, *op. cit.*, p. 3.

30 *Ibidem*.

31 Cfr. A. Simoncini, S. Suweis, *op. cit.*, p. 92.

32 Cfr. *ibidem*.

33 Si veda M. Lindstrom, *Small Data: i piccoli indizi che svelano grandi trend*, Milano, 2016. Secondo Lindstrom, l'osservazione dei comportamenti delle persone, delle loro azioni quotidiane e di *routine* nel loro ambiente naturale, piuttosto che all'interno di un *database*, può rivelarsi maggiormente significativa con riguardo ai processi decisionali soggettivi.

34 Cfr. S. Palanza, *op. cit.*, p. 7.

35 Cfr. M. Orefice, *op. cit.*, p. 62.

36 Cfr. *ibidem*.

inefficaci della penuria di informazioni[37]. D'altro canto, la repentina evoluzione economica e sociale richiede agilità di mezzi e, in tale contesto, sfruttare adeguatamente la potenziale ricchezza informativa costituisce un indubbio vantaggio competitivo, fattore che motiva, in genere, la diffusa contrarietà imprenditoriale verso alcune politiche sulla portabilità dei dati[38]. Per trasformare i dati in informazioni significative si utilizzano tecniche informatiche come, ad esempio, il *Data Mining*, procedimento di estrazione della conoscenza da banche dati di grandi dimensioni, mediante l'applicazione di algoritmi che individuano ed esplicitano le associazioni tra i dati[39]. Il *Data Mining* costituisce, in altre parole, un procedimento all'interno del quale si utilizzano una o più tecniche per estrarre conoscenza da grandi quantità di dati, in termini di associazioni, *pattern*, regole, o sequenze ripetute[40], consentendo, successivamente, di incrociare i dati personali in modo da estrarne tendenze e convergenze che coadiuvano, innanzitutto, il settore del *marketing* nella fidelizzazione della clientela[41]. Tale percorso conoscitivo viene, al momento, proseguito dalla *Business Analytics*, sommariamente definibile qui come l'insieme degli strumenti e delle applicazioni *software* di accesso, di analisi e di visualizzazione dei dati che aiutano il *management* a cogliere rapidamente le informazioni di rilievo e a controllare le prestazioni aziendali, nell'assumere le più efficaci decisioni. Attraverso tali procedure di ricerca e di estrazione di informazioni utili da grandi quantità di dati, mediante metodi automatici o semi-automatici ed il loro utilizzo principalmente aziendale e industriale, gli individui sono progressivamente assimilati a sensori nell'ambiente[42], condizione accentuata dal progressivo affermarsi dell'*Internet of Things*, a cui occorre, ora, accennare.

L'*Internet of Things* e le tecnologie di identificazione a radiofrequenza

L'*Internet of Things* (IoT), espressione coniata dal ricercatore britannico Kevin Ashton nel 1999, esprime il passaggio da una rete di *computer* interconnessi ad una rete di oggetti della vita quotidiana in connessione, facilitato dallo sviluppo della tecnologia *wireless* e satellitare che consente di gestire efficacemente una mole crescente di informazioni[43]. Siamo di fronte, in altri termini, al fenomeno di oggetti di uso quotidiano "intelligenti", ovvero, capaci di interagire fra di loro e con gli utenti, sviluppando le potenzialità insite nella Rete in direzione di innovative applicazioni delle informazioni provenienti dall'ambiente[44]. I più recenti sviluppi dell'*Internet of Things* segnano un'ulteriore evoluzione determinata dal tentativo di connessione di ogni oggetto esistente: per tale ragione si parla di *Internet of Everything* (IoE), fenomeno che futuristicamente, ma neanche tanto, vedrebbe in collegamento persone, dati e procedure utilizzando sistemi capaci non solo di memorizzare, ma altresì di apprendere e di generare informazioni[45]. L'identificazione degli oggetti interconnessi – avvalendosi della combinazione di sensori e di meccanismi di riconoscimento au-

37 Cfr. ad esempio, *Profilazione 2.0: dimmi come clicchi e ti dirò chi sei*, in: www.MyMarketing.net del 24.09.2010.

38 Cfr. M. Orefice, *op. cit.*, p. 62.

39 Cfr. *Data Mining*, in: https://www.cineca.it. Sull'impiego delle reti neurali e sull'utilizzo degli algoritmi di apprendimento, supervisionato e non supervisionato, si veda A. C. Amato Mangiameli, *Algoritmi e big data*, cit., p. 108. Sul funzionamento delle reti neurali, cfr anche G. De Anna, *Automi, responsabilità e diritto*, in: "Rivista di filosofia del diritto", VIII (2019), n. 1, p. 131.

40 *Data Mining*, in: https://www.cineca.it.

41 Cfr. alla url http://open.cineca.it/datamining/db__marketing/db__marketing.htm, p. 2. Per un'analisi delle criticità del *Data Mining*, C. Sarra, *Business Intelligence ed esigenze di tutela: criticità del c.d. Data Mining*, in: P. Moro, C. Sarra, (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Milano, 2017, pp. 41-63.

42 Cfr. D. Talia, *op. cit.*, p. 81.

43 Cfr. S. Palanza, *op. cit.*, p. 2.

44 Tale processo sottende la presenza di un oggetto il quale, mediante sensori connessi alla rete ed eventualmente ad altri oggetti *smart*, riceve dall'ambiente degli *input* che comunicano i dati acquisiti ad un *server* che, dopo averli opportunamente elaborati, invia dei comandi all'oggetto in questione facendo sì che questi risponda con degli *output*, cfr. ivi, p. 3.

45 Cfr. S. Palanza, *op. cit.*, p. 6.

tomatico - avviene frequentemente tramite un identificativo univoco, ad esempio un numero di serie, riconoscibile in radiofrequenza[46]. L'identificazione a radiofrequenza (RFID) si basa sull'utilizzo di microprocessori collegati ad un'antenna, impiegati come etichette di riconoscimento - *etichette intelligenti* – e in grado di trasmettere, mediante onde radio, segnali leggibili da appositi lettori[47]. E' opportuno rilevare come, attraverso le etichette intelligenti, si possano trattare, in alcuni casi anche senza che il soggetto interessato ne sia a conoscenza, molteplici dati personali, comprese informazioni di natura sensibile che, in un secondo momento, potrebbero essere aggregate ad altre consentendo una più o meno delineata profilazione dell'interessato[48]. Gravi incognite sulla tutela della riservatezza individuale derivano, altresì, dal prevedibile incremento della potenza dei sistemi di identificazione a radiofrequenza - ad esempio con una lettura delle etichette a maggiori distanze - nonché dalla possibilità che terzi non autorizzati, agevolati dall'adozione di *standard* tecnici comuni, leggano i contenuti delle etichette o intervengano sulle stesse mediante la loro riscrizione[49]. Al riguardo, il Garante con il provvedimento 09/03/2005, concernente le garanzie nell'utilizzo delle etichette intelligenti, ha rilevato l'impatto che le tecniche di identificazione a radiofrequenza possono avere sull'esercizio dei diritti di libertà individuale e sulla tutela dei dati personali coinvolti in tale genere di elaborazione elettronica. Su questi temi si è anche espressa, già da tempo, la Commissione delle Comunità europee con la Comunicazione del 15 marzo 2007 delineando una linea politica che ha come obiettivo la difficile conciliazione tra un'opportuna valorizzazione delle tecnologie attualmente a disposizione e la tutela della privacy, sottolineando i rischi per la salute e per l'ambiente derivanti dall'impiego delle stesse[50]. Va poi segnalato come le RFID vedano, negli ultimi anni, soprattutto grazie alla diffusione degli *smartphone*, il massiccio utilizzo delle *Near Field Communication* (NFC), tecnologie che forniscono una connettività *wireless* bidirezionale e a corto raggio[51]. Le NFC, nel consentire una crescente interazione dei sensori con l'ambiente, rappresentano un'incognita soprattutto con riguardo alle dovute garanzie di riservatezza nel trattamento dei dati personali. Al riguardo, è da menzionare l'Opinion 8/2014 *On the Recent Development on Internet of Things* del WP29 (*Article 29 Data Protection Working Party*) che individua gli sviluppi dell'*Internet of Things*, ne riconosce l'invasività e la necessità di anonimizzare alcune informazioni, eccettuate le situazioni nelle quali si renda strettamente necessaria l'identificazione degli interessati[52]. La convergenza degli oggetti connessi in rete rende, come si è visto, la

46 Cfr. M. Iasselli, Privacy e nuove tecnologie, in M. Iasselli (a cura di), *Diritto e nuove tecnologie. Prontuario giuridico ed informatico*, Milano, 2016, pp. 153.

47 Cfr. ivi, p. 135. La tecnologia dell'identificazione a radiofrequenza, secondo la definizione offerta dalla Raccomandazione 2009/387/CE, esprime "l'uso di onde elettromagnetiche o l'accoppiamento di un campo reattivo nella porzione di radiofrequenza dello spettro per comunicare a partire da, o verso, un'etichetta mediante una varietà di sistemi di modulazione e codifica allo scopo di leggere, in modo univoco, l'identità di un'etichetta di radiofrequenza o altri dati in essa registrati". Per un utile approfondimento, cfr. G. Pascuzzi, *op. cit.*, pp. 73-74.

48 Cfr. M. Iasselli, *op. cit.*, p. 135.

49 Cfr. ivi, p. 136.

50 Si fa riferimento alla Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, della Commissione delle Comunità Europee, del 15/03/2007, "L'identificazione a radiofrequenza (RFID) in Europa: verso un quadro politico". Nel settore sanitario, si può ricordare l'intervento dell'Autorità Garante del 29/11/2012, effettuato in sede di verifica preliminare richiesta da un'azienda ospedaliera in materia di trattamento dei dati personali attraverso Rfid per il monitoraggio a distanza di pazienti portatori di defibrillatori cardiaci impiantabili attivi. In tale sede, il Garante - richiamando il provvedimento del 9/03/2005 sulle garanzie da assicurare ai soggetti interessati nel caso di utilizzo delle "etichette intelligenti" – precisa come l'inserimento sottopelle di microprocessori, per l'evidente delicatezza della situazione e delle ricadute sui diritti soggettivi coinvolti, renda necessaria la predisposizione di peculiari cautele dovendo effettuarsi in stretta aderenza al principio di proporzionalità, espresso dall'art. 11 del Codice Privacy, nonché salvaguardando la dignità dei soggetti interessati, come previsto dall'art. 2 del Codice Privacy.

51 Cfr. S. Palanza, *op. cit.*, pp. 18 sgg.

52 Cfr. *ibidem*.

diffusione delle informazioni personali sempre più pervasiva e, a tale condizione, spesso si aggiunge il mancato controllo dell'individuo del flusso di dati generato dal dispositivo utilizzato, frequentemente causato da una sua attivazione improvvisa[53]: ne deriva, oltre all'aumento dei dati trasmessi *online*, la nascita di nuove modalità di minaccia alla privacy, rese possibili da un anonimato sempre più difficile da mantenere nel *Web* e dalla pressoché automatica identificazione dei profili individuali[54]. Per tali ragioni, considerate le prolematiche implicate tanto nella raccolta come nel trattamento dei dati personali, la giurisprudenza statunitense – tendente a considerare la protezione dei dati personali da una prevalente ottica di mercato, sottovalutandone il loro coinvolgimento nell'esercizio di diritti fondamentali[55] - ha elaborato il principio della *reasonable expectation of privacy*, secondo il quale le violazioni alla privacy sarebbero da rapportare al livello di riservatezza ragionevolmente esigibile nel caso concreto, esaminandone il *potenziale di invadenza* nelle relazioni umane[56]. Oggi, tuttavia, diventa sempre più complesso stabilire sino a che punto può ragionevolmente spingersi l'aspettativa di privacy, nella ferma necessità di frenare l'indiscriminato trasferimento dei dati personali che costituiscono e custodiscono il fulcro di diritti fondamentali[57]. Oltre all'eterogeneità degli strumenti connessi in Rete va, poi, considerata la molteplicità dei soggetti che, a vario titolo, ruotano intorno al mondo della raccolta, dell'elaborazione e dell'archiviazione dei dati personali: dalla Pubblica Amministrazione alle aziende private, dai gestori dei *social network* fino ai motori di ricerca[58]. Tra le figure professionali coinvolte, spicca il ruolo dei *data brokers*, rivenditori di dati ai soggetti finali[59], che operano raccogliendo informazioni idonee ad identificare gli individui, da suddividere in *data segments*, dando luogo, in modo sempre più capillare e grazie ad un'opportuna combinazione dei dati raccolti con efficaci modelli predittivi, a dettagliate segmentazioni dei modelli di riferimento[60]. Queste prime considerazioni evidenziano come l'analisi dei dati, ottenuti in primo luogo tramite gli oggetti *smart*, rappresenti una vera e propria sfida da cogliere e mostrano come la necessità di una regolamentazione, riguardante il flusso informativo, sia impellente[61]. Altrettanto indifferibile è un'attenta considerazione giuridico-normativa del fenomeno in questione e della sua portata transnazionale che si proponga di delineare un riferimento unitario per i soggetti interessati, nella primaria considerazione della tutela dei diritti fondamentali, sebbene "la storia dei diritti dell'uomo, meglio non farsi illusioni, è quella dei tempi lunghi"[62].

I *Big Data*: condivisione della conoscenza e tutela delle informazioni personali

L'uso cooperativo e partecipato nella sfera pubblica di alcune tipologie di Big Data riveste un sicuro interesse sociale. E' questo il caso della condivisione di informazioni riguardanti il traffico cittadino, rivolta ad ottenere l'indispensabile conoscenza che consenta di trasformare una città in una *smart city*, come anche il caso del monitoraggio dei dati riguardanti il traffico e l'inquinamento, finalizzato ad implementare la tutela del territorio ed ambientale, ma è, soprattutto, quello scientifico il contesto dove i Big Data e la loro condivisione assumono una rilevanza determinante, poiché fondamentale appare la messa in comune delle ri-

53 Cfr. ivi, p. 15.

54 Cfr. *ibidem*.

55 Cfr. ivi, p. 12.

56 Cfr. M. Calvo, F. Ciotti, G. Roncaglia, M. A. Zela, *Internet 2004. Manuale per l'uso della Rete*, Roma-Bari, 2003, pp. 585-86.

57 Cfr. M. Orefice, *op. cit.*, p. 141.

58 Per un approfondimento delle figure coinvolte nella tutela della privacy, si veda M. C. De Vivo, *Privacy: la legislazione, le imprese, la P. A. e la formazione in Italia. Intervista a Maria Concetta De Vivo*, del 16 dicembre 2013, in: http://www.alavie.it.

59 Cfr. M. Delmastro, A. Nicita, *op. cit.*, pp. 39-41.

60 Cfr. *ibidem*. Sulla funzione dei data broker e sulla cosiddetta infonomics, economia dell'informazione, cfr. D. Talia, *op. cit.*, pp. 60 sgg.

61 S. Palanza, *op. cit.*, p. 4.

62 N. Bobbio, *op. cit.*, p. 264.

cerche scientifiche e dei loro esiti[63]. I Big Data "stanno prendendo la scena mondiale come una delle discipline più potenti e affascinanti di tutti i tempi, principalmente per le opportunità che offrono in tutti i campi, dalla politica all'economia, nelle ricerche sociali, nella cultura e in tutta la ricerca scientifica"[64]. La raccolta e il monitoraggio dei Big data assume, in questi ambiti, una valenza estremamente positiva vedendo le informazioni raccolte declinate a favore della condivisione della conoscenza e dell'eguaglianza[65], a fondamento della partecipazione democratica che vorrebbe – come ricordano l'art. 19 della Dichiarazione Universale dei Diritti dell'Uomo, nonché l'art. 21 della nostra Costituzione - l'accesso alle conoscenze e alla cultura libero e giuridicamente garantito[66]. Oltre ai menzionati vantaggi economici e sociali, è opportuno, tuttavia, rilevare alcune delle principali criticità emergenti dall'utilizzo dei Big Data e concernenti, innanzitutto, la tutela dei dati personali.

L'economia dell'informazione e lo sfruttamento economico dei dati personali

Per quanto concerne lo sfruttamento economico dei dati personali, ci si domanda se, con il rilascio del consenso all'utilizzo degli stessi, - che spesso avviene da parte dell'interessato in maniera del tutto automatica, se non proprio inconsapevole - si assista o meno ad un congiunto passaggio del diritto di proprietà sul dato personale o se la manifestazione del consenso non rappresenti, piuttosto, una delega all'impiego esclusivo del dato, funzionale ad individuare il titolare delle informazioni e a permettere l'erogazione del servizio[67]. Infatti, "c'è una certa differenza tra la consapevolezza di esprimere un consenso 'formale' a utilizzare il proprio dato e quella di partecipare ad una vera e propria transazione economica sul proprio dato"[68]. Tale ambiguità fa sorgere improrogabili domande sull'effettività della tutela della privacy digitale, nonché sul dovuto rispetto della concorrenza tra gli operatori del settore, fattore che incide significativamente nella regolazione dei mercati. Nel caso in cui si propenda per l'ipotesi di cessione di una delega esclusiva, si può, infatti, notare come quest'ultima, se da un lato eviti l'indiscriminata circolazione delle informazioni personali, prevenendo un possibile mercato dei dati, al contempo permetta un utilizzo monopolistico dell'informazione nella piattaforma *online*. "Il bene pubblico (l'informazione) diventa un bene privato proprietario *de facto*, ma solo per la piattaforma che lo utilizza (...). L'uso congiunto di più piattaforme online da parte degli utenti (*multihoming*) potrebbe in parte, e sotto certe condizioni, mitigare questo fenomeno"[69]. In base a tali considerazioni, la strada da percorrere potrebbe essere quella di un superamento del principio della delega esclusiva in favore del trasferimento di un diritto proprietario riguardante solo alcuni utilizzi del dato personale, facendo sì che determinate informazioni rimangano circoscritte alla sfera più riservata, mentre altre vengano pubblicamente condivise[70]. Al riguardo, il riconoscimento del diritto alla portabilità dei dati personali, sancito dall'art. 20 del GDPR, sembra corrispondere a questa logica, da applicare anche ai dati non strutturati i quali non richiederebbero alcuna manifestazione di consenso poiché la loro estrazione avviene al di fuori di una specifica transazione[71]. Va evidenziato come la cessione del dato e la sua valorizzazione economica non rilevino solo in riferimento alla tutela della privacy, ma anche al fine della

63 Cfr. S. Palanza, *op. cit.*, p. 128.

64 F. Casi, *op. cit.*, p. 3.

65 Sulle potenzialità dei *Big Data*, utilizzabili nella prevenzione delle violazioni dei diritti umani, si veda L. Nosari, *Potenzialità e problematiche afferenti l'utilizzo dei Big Data in materia di diritti umani*, in: https://www.cyberlaws.it.

66 J. Drexl, *Economic efficiency versus democracy: on the potential role of competition policy in regulating digital markets in times of posttruth politics*, in: Max Plank *Institute for Innovation and Competition Research*, dicembre 2016, paper n. 16, pp. 1-28.

67 Cfr. M. Delmastro, A. Nicita, *op. cit.*, p. 30.

68 Ivi, p. 42-43.

69 Ivi, p. 127.

70 Cfr. ivi, p. 128.

71 Cfr. ivi, pp. 129-30.

costruzione giuridica, oltre che economica, di un mercato trasparente dei dati[72] e, a tal proposito, va ricordato come il GDPR abbia significativamente rafforzato gli obblighi di trasparenza nei processi di acquisizione e di trattamento dei dati personali.

Consapevolezza e libertà nella manifestazione del consenso

Altra complessa e rilevante problematica riguarda, poi, la difficoltà nello stabilire quando e quanto l'utente sia effettivamente consapevole della raccolta dei dati personali e del loro trattamento[73] - considerato che non sempre l'accesso ad un dato specifico è condizione indispensabile per la fruizione di un servizio - anche alla luce di meccanismi informatici, quali i *tracking walls*, che possono escludere da un determinato servizio gli utenti che rifiutino di estendere il consenso ad esso fornito anche ad un'altra prestazione[74] o che agiscono come fattori di marginalizzazione e di forzatura del consenso, come avviene nel caso del *devices tracking*[75]. In queste ipotesi, l'accettazione, apparentemente libera, degli utenti consente alle aziende di sfruttare le informazioni personali, ponendo gravi interrogativi sulla tutela della riservatezza e sulla libertà di espressione, in quanto, per "nascondersi" l'individuo potrebbe, in *extrema ratio*, rinunciare alla libertà di scegliere i contenuti a cui accedere e i siti da visitare in Rete[76]. In tal caso, il rifiuto di fornire le proprie informazioni "implicherebbe l'esclusione da un numero crescente di processi sociali, dall'accesso alle conoscenze alla fornitura di beni e servizi"[77]. Tali pratiche, seppur diffuse, si pongono in contrasto con l'art. 4 del GDPR concernente il consenso informato - non essendo, infatti, conforme al Regolamento una richiesta che accorpi finalità disomogenee o che impedisca o disturbi la fruizione di un servizio offerto *online* – nonché con il requisito della libertà del consenso, visto che quest'ultimo non può dirsi effettivamente libero quando la sua cessione costituisca il prezzo del sevizio[78]. Come ha sottolineato, nell'ottobre del 2014, Margaret Vestager, Commissario Europeo per la concorrenza, i dati costituiscono la nuova moneta di Internet e, di conseguenza, non possono essere definiti come *free* - termine che rimanda al concetto di gratuità e di libertà - i servizi *online* ottenuti tramite la cessione dei dati personali. I dubbi in merito alla libertà nella cessione del consenso s'intensificano ulteriormente se solo si consideri l'attuale indispensabilità di alcuni servizi nelle comunicazioni interpersonali. "Quello che ci sembra un banale strumento per ottenere un libero accesso è in realtà il vero bene, il cui scambio regge la transazione commerciale sottostante. Lo *scambio implicito*, per tutta questa gratuità di servizi, è con la nostra attenzione, con il rilascio di dati che permetteranno poi promozioni e pubblicità personalizzate per i nostri bisogni. A questo scambio implicito corrisponde un *mercato implicito*, quello dei dati, del quale sappiamo ancora troppo poco. Come spesso si ripete in questi casi, il *prodotto siamo noi*"[79]. E' da dotare come il Regolamento europeo non faccia diretta menzione dei Big Data, escludendo inspiegabilmente dati quotidianamente raccolti ed incrociati, in grado di restituire informazioni talvolta più che sensibili sull'individuo e capaci di incidere profondamente sull'esplicarsi delle libertà fondamentali. Di conseguenza, si può comprendere come le informative per la cessione del consenso, seppure strutturate in maniera conforme al Regolamento del 2016, non sembrino sufficientemente efficaci nell'arginare il sempre maggiore utilizzo dei Big Data immessi nel mercato[80] e del loro potenziale pre-

72 Ivi, p. 31.

73 Si veda A. C. Amato Mangiameli, *Algoritmi e big data*, cit., p. 112.

74 Cfr. A. C. Zanuzzi, *Internet of things e privacy. Sicurezza e autodeterminazione informativa*, in: P. Moro, C. Sarra (a cura di), *Tecnodiritto*, cit., p. 115.

75 Cfr. ivi, pp. 116-18.

76 Cfr. M. Orefice, *op. cit.*, pp. 106-107; cfr. S. Rodotà, *Il mondo nella rete*, cit., p. 26.

77 Ivi, p. 29.

78 Cfr. M. Orefice, *op. cit.*, pp. 110-111.

79 M. Delmastro, A. Nicita, *op. cit.*, p. 24.

80 Cfr. ivi, p. 117. Gli OTT, piuttosto che adeguarsi alle disposizioni del Regolamento del 2016 e nell'assenza

dittivo, aggirando il perimetro delle norme sul consenso al trattamento dei dati personali[81] e prestandosi ad applicazioni per lo più formalistiche[82]. Va, in ogni caso, considerato come il quadro legislativo europeo, pur non contemplando direttamente i Big Data, stabilisca comunque alcuni principi fondamentali nella raccolta e nell'utilizzo delle informazioni personali, e come recenti sentenze della Corte di giustizia dell'Unione europea ricordino l'importanza di un'efficace protezione dei dati[83]. Il Garante europeo, infine, in diversi pareri e iniziative, non ha mancato di sottolineare il rilievo di una coerente applicazione normativa nell'epoca dei Big Data, elaborando il concetto di *protezione* delle informazioni personali e sottolineando la necessità di cogliere le opportunità offerte dalle nuove tecnologie, senza consentire loro di determinare i valori sociali di riferimento[84]. "Il reale problema nasce dalla scarsa coscienza che i cittadini hanno di quanta parte della loro privacy sia in vendita, di quanto sia invasiva nelle loro vite la pubblicità personalizzata costruita sui loro clic e di quanto sia inadeguata la difesa che i sistemi legislativi attuali realmente garantiscono a tutela dei cittadini e delle comunità"[85]. La mancanza di una piena consapevolezza potrebbe, altresì, riguardare l'esistenza di *second* (o *subsequential*) *uses* dei propri dati, come anche riferirsi alle *secondary informations* sollecitate dalle tecniche di estrazione di informazioni significative dai dati, in grado di generare informazioni differenti da quelle oggetto del trattamento originario ed utilizzate per finalità ulteriori rispetto a quelle espresse da quest'ultimo le quali, ove sconosciute all'interessato, risulterebbero illecite, poiché non espressamente autorizzate[86]. Per ciò che riguarda i *second uses* dei dati personali occorrerà, dunque, prestare un consenso specifico al loro trattamento, a testimonianza di una completa consapevolezza e della volontà di autorizzazione a che il trattamento venga posto in essere: diversamente, le operazioni di trattamento sui dati personali dovranno ritenersi illecite ponendosi in contrasto con l'art. 13 0, se dati sensibili, con l'art. 26 del d. lgs. 2003/196 (Codice Privacy) e con gli artt. 13, 7, e 9 del Regolamento europeo 2016/679[87].

Nel settore dell'*Internet of Things* è, poi, concreto il rischio di attivazione involontaria del dispositivo *smart* e, conseguentemente, di cessione inconsapevole del flusso di dati da esso generato, con un'evidente perdita del controllo informativo e del potere decisionale sulle informazioni personali da parte dell'utilizzatore[88]. Di grande interesse appare, allora, la citata Opinion 8/2014 del WP29 laddove precisa che, affinché il trattamento possa considerarsi lecito è necessario che lo *user* rimanga nel pieno controllo dei propri dati per tutto il ciclo vitale del dispositivo[89]. In riferimento all'IoT e alle tecnologie informatiche in grado di attivare una profilazione individuale invasiva – tale da riguardare anche i dati sensibili degli utilizzatori[90] - l'incertezza normativa pare, tuttavia, accentuarsi visto che ai trattamenti di dati per-

di sanzioni penali, la cui previsione è rimessa alla discrezionalità degli Stati membri, potrebbero preferire la comminazione di sanzioni amministrative pecuniarie, perseverando nella condotta scorretta, cfr. *ibidem*.

81 Cfr. F. Casi, *op. cit.*, p. 1.

82 Cfr. M. Delmastro, A. Nicita, *op. cit.*, p. 142.

83 Si veda la seduta plenaria del Parlamento europeo, marzo II 2017, *Implicazioni dei Big Data per i diritti fondamentali*, nonché la risoluzione del Parlamento europeo del 14 marzo 2017 *Implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto*, in: www.europarl.europa.eu.

84 Si veda, ancora, la seduta plenaria del Parlamento europeo, marzo II 2017, *Implicazioni dei Big Data per i diritti fondamentali*, cit.

85 D. Talia, *op. cit.*, p. 48.

86 Cfr. A. C. Zanuzzi, *op. cit.*, pp. 111-12.

87 Cfr. ivi, pp. 112-13.

88 Cfr. ivi, p. 110.

89 Cfr. *ibidem*. Il WP29 distingue il trattamento di dati consistente nella loro acquisizione da parte del produttore del *device*, o di diverso *stakeholder*, da quello connesso ad un loro eventuale successivo utilizzo, cfr. ivi, p. 113.

90 È il caso dell'utilizzo di un navigatore capace di rilevare i luoghi frequentati e i tragitti percorsi, informazioni da utilizzare, successivamente, in vista dell'invio di comunicazioni commerciali mirate sulle preferenze e sulle abitudini dello *user*; si pensi, altresì, ai dispositivi inseriti nelle automobili in grado di rilevare la stanchezza del conducente mediante la processazione dei dati del volto e alla possibilità di inviare tale informazioni a soggetti terzi, cfr. ivi, p. 111.

sonali, connessi alla fornitura di servizi di comunicazione elettronica, andrebbe applicata la Direttiva 2002/58 (Direttiva *ePrivacy* relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche) [91] le cui disposizioni – recepite agli artt. 32 e 32 bis e 121-132 del Codice privacy - sono attualmente in corso di revisione essendo stata presentata una proposta di Regolamento finalizzata alla loro abrogazione[92]. Nell'attuale fase interlocutoria, caratterizzata da ampi margini di incertezza, almeno fino a quando non verrà alla luce il testo definitivo del documento, si potrà, ancora, guardare all'Opinion 8/2014 del WP29 la cui portata di principio in materia di trattamento dei dati personali rimarrà, comunque, immutata indipendentemente dalla direzione che verrà indicata dal nuovo dettato normativo[93]. Secondo il WP29, le criticità menzionate potrebbero essere riferite tanto alla natura del *device* degli oggetti *smart* come ad un difetto di coordinamento tra gli *stakeholders* nel trattamento dei dati personali, in relazione all'adozione delle necessarie misure minime di sicurezza[94]. Nella prima ipotesi, ci si potrebbe appellare al necessario rispetto del criterio della *privacy by design*, ovvero, della "protezione dei dati fin dalla progettazione", espresso dall'art. 25 del Regolamento UE 2016/679, che anticipa la tutela dei dati personali fin dalla progettazione del trattamento, mediante un approccio proattivo e non meramente reattivo: tale indicazione appare essenziale in relazione ai trattamenti effettuati con gli oggetti *smart* poiché rende la tutela dei dati personali una componente intrinseca della struttura architettonica del *device*. Al riguardo, va altresì menzionato l'art. 32 del Codice privacy che obbliga i fornitori di servizi di comunicazione elettronica ad adottare le "misure tecniche e organizzative adeguate al rischio esistente per salvaguardare la sicurezza dei suoi servizi e per gli adempimenti di cui all'art. 32 *bis*" (cioè per le notificazioni in caso di *data breach*). Nella medesima linea di garanzia delle informazioni personali, si pone anche l'art. 24 del Regolamento UE 2016/679, riferito al principio di *accountability* - di ardua traduzione in lingua italiana, ed espresso con il termine della "responsabilità"[95] – riferito al complesso delle misure che il titolare e il responsabile del trattamento devono porre in atto per "garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al presente regolamento", criterio sorto con specifico rimando alle informazioni economico-finanziarie e consuntive, ma idoneo ad investire la globalità delle operazioni aziendali. Alla garanzia della *privacy by design* e al principio di *accountability* si affianca, poi, il rispetto della *privacy by default*, recepito dall'art. 25 del Regolamento, che prevede che vengano trattati per impostazione predefinita solo i dati personali necessari e sufficienti ad ogni specifica finalità di trattamento e per il periodo strettamente necessario a tali fini[96]. Tale principio esprime un'efficace protezione "contro il rischio, particolarmente insidioso e presente negli oggetti *smart*, di utilizzazione dei dati effettuata da un numero indefinito di soggetti e per finalità diverse da quella per le quali essi sono stati originariamente raccolti, tanto più se perseguito in

91 Sul tema è intervenuta la Direttiva 2009/136 il cui considerando n. 56 stabilisce che "quando tali dispositivi (RFID) sono collegati a reti di comunicazione elettronica accessibili al pubblico o usano servizi di comunicazione elettronica come infrastruttura di base è opportuno che si applichino le disposizioni pertinenti della Direttiva 2002/58/CE".

92 "Proposta di Regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58 CE (Regolamento sulla vita privata e le comunicazioni elettroniche)"; sull'argomento, cfr. A. C. Zanuzzi, *op. cit.*, p. 101.

93 Cfr. ivi, p. 102.

94 Cfr. ivi, pp. 103-106.

95 In ambito pubblicistico, il concetto di *accountability* viene spesso collegato a quello di trasparenza dato che, nel compiere atti di rilevanza per la comunità nazionale, le pubbliche istituzioni si assumono una responsabilità della quale i cittadini possono chiedere un riscontro formulando domande e osservazioni sul rendimento degli uffici pubblici e dei loro dirigenti. L'*accountability* si compone di tre elementi: la *trasparenza* quale garanzia di accessibilità alle informazioni, principalmente da parte dei cittadini; la *responsività*, da intendersi come capacità di rendere conto di scelte e di condotte agli *stakeholder*; la *compliance*, quale capacità di far rispettare le norme nell'azione pubblica come nella pratica degli operatori di settore, cfr. M. Iasselli, *op. cit.*, pp. 180-81.

96 Cfr. *ibidem*.

modo automatizzato e senza l'individuazione di una chiara responsabilità riconducibile ad un titolare individuato"[97]. Ai criteri menzionati si può, infine, affiancare il Considerando 78 del Regolamento europeo del 2016 il quale dispone che "la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento (...). Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonomizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento dei dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare le caratteristiche di sicurezza". La suddetta disciplina resterà centrale anche dopo l'entrata in vigore della *eRegulatio*n poiché quest'ultima, non contenendo una regolazione generale delle misure di sicurezza, rinvierebbe, in ogni caso, a quella contenuta nel Regolamento 2016/679 e nel Codice UE delle comunicazioni. La sfida è quella di armonizzare interessi e necessità spesso contrastanti, quali la trasparenza e la riservatezza, riuscendo ad anonimizzare gli utenti senza cancellare l'interesse dei dati raccolti[98], ottenendone un adeguato bilanciamento tra le logiche di mercato e l'imprescindibile garanzia di diritti prevalenti e non negoziabili[99].

I *Big Data* e la polarizzazione dell'informazione

Un'ulteriore incognita - che ha dato vita ad un acceso dibattito da parte di Parlamenti, Governi, Autorità garanti della tutela della concorrenza, della privacy digitale e della *cyber security* – determinata dal crescente utilizzo dei Big Data, è data dalla progressiva concentrazione dell'informazione in capo a pochi operatori, fenomeno che necessariamente si riflette sulla piena esplicazione dei diritti di libertà e, in definitiva, sul futuro della democrazia. Le piattaforme globali, in grado di raccogliere, elaborare e utilizzare le informazioni provenienti dai Big Data, denominate *Over the Top* (OTT) o "giganti digitali", *Big Tech*, rappresentano, infatti, soggetti capaci di sviluppare servizi gerarchicamente al di sopra delle tradizionali infrastrutture fisiche delle telecomunicazioni fisse e mobili di accesso alla Rete e, pertanto, in grado di affermare un'inedita intermediazione tra i versanti del mercato, fondata su una struttura tecnologica ad altissima intensità e basata, per quanto concerne l'utilizzo dei dati, su modelli di integrazione verticale[100]. In altri termini, ciò comporta che i dati, una volta acquisiti, vengono gestiti internamente e prevalentemente dalle piattaforme digitali, dando luogo ad una spiccata polarizzazione informativa. "Lasciare al mercato il governo dell'economia dei dati significa affidarsi alle regole private dell'intermediazione centralizzata delle grandi piattaforme *online* che cattura, e gestisce in proprio, l'informazione rilevata dai diversi soggetti intermediati a vario titolo"[101]. Tale processo di concentrazione dell'informazione sembra porsi contro il principio di uguaglianza, che si traduce qui nella pretesa dei cittadini di avere un effettivo controllo sui propri dati personali, e contro la tutela della concorrenza, visto che i dati raccolti dagli OTT diventano di dominio esclusivo di pochi *players*, in grado di porre barriere di ingresso a nuovi *competitors*, falsando il gioco della concorrenza, anche a danno del consumatore[102]. La titolarità dei dati sembrerebbe, quindi, imporsi quale *essential facility* di carattere immateriale, indispensabile per competere sul mercato, facendone discendere l'obbligo di aprire i dati in capo ai giganti dell'informazione[103]. Da quest'ottica, "i *Big Data* diventano il nocciolo duro delle libertà fonda-

97 F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, 2016, p. 288.

98 Cfr. M. Orefice, *op. cit.*, p. 121.

99 Cfr S. Rodotà, *Il mondo nella rete*, cit., pp. 21 sgg.

100 Cfr. M. Delmastro, A. Nicita, *op. cit.*, p. 51-53.

101 Ivi, p. 125.

102 Cfr. M. Orefice, *op. cit.*, p. 11. Sulle pratiche anticoncorrenziali nello sfruttamento abusivo della posizione dominante, con particolare riferimento a *Google*, cfr. ivi, pp. 191-195 e pp. 214-27.

103 Cfr. ivi, p. 13.

mentali, ma si tratta di un nucleo bifronte: da un lato la loro conoscenza è precondizione per l'esercizio delle libertà fondamentali (...) dall'altro i *Big Data* rappresentano l'intimità più profonda della persona, in grado di rilevare informazioni sull'individuo riservate che, in quanto tali, devono essere protette, anonimizzate e minimizzate in modo che la persona cui si riferiscono non sia identificabile"[104]. In prospettiva, ed in accordo con quanto stabilito dall'art. 21 della Carta Costituzionale sulla libertà di manifestazione del pensiero, emerge la necessità di valutare l'accesso ad Internet come un diritto fondamentale della persona e di considerare la conoscenza come bene pubblico globale, evitando, al di là di precise ipotesi previste a tutela della privacy, ogni possibile fenomeno di chiusura dell'informazione, capace di trasformare un bene fruibile in risorsa limitata[105]. Ciò segnerebbe un importante passo verso una conoscenza condivisa e un mondo propriamente interattivo, inaugurando un efficace modello di cittadinanza digitale e generando una nuova forma di solidarietà civile alimentata dall'informazione[106].

I *Big Data* tra algoritmi e democrazia

La capacità di influenza delle piattaforme *online*, diretta, in primo luogo, a fini di *marketing*, appare altrettanto efficace nel contesto politico potendo queste ultime, quali intermediari digitali dell'informazione, influenzare le scelte dei cittadini, giungendo persino, in taluni casi, a distorcere l'organizzazione gerarchica (*ranking*) delle notizie in ricerca, soprattutto in periodo elettorale. Evidente è, in queste circostanze, il rischio rappresentato dai latifondisti della conoscenza[107] nell'inviare messaggi mirati e parziali, frequentemente selezionati tramite la cosiddetta *Sentiment analysis*[108] e prediligendo la pratica del *clickbaiting*, cioè, l'utilizzo di titoli-esca realizzati per attirare *click* e suscitare la visualizzazione di pagine *Web*, capaci di incidere sul libero agire del singolo e di porre

104 Ivi, p. 165-66.

105 Cfr. S. Rodotà, *Il mondo nella rete*, cit., p. 72.

106 Cfr. M. Orefice, *op. cit.*, p. 25. In Italia il D. lgs. 25 maggio 2016, n. 97 ha introdotto il cosiddetto accesso generalizzato, subordinato alla richiesta del cittadino, cioè, alla domanda di accesso, cui segue, indirizzata al singolo utente che ne ha fatto richiesta, l'eventuale risposta dell'Amministrazione statale. Tale procedimento si rivela, dunque, distante dall'*Open Data policy* e dalla piena attuazione del principio di trasparenza, quale espressione democratica, in grado di alimentare un rete di condivisione, interoperabilità e riutilizzo della conoscenza, cfr. ivi, pp. 46 73. Sul recepimento del paradigma *open* nell'ordinamento giuridico italiano, cfr. ivi, pp. 29 sgg. Sulle più rilevanti problematiche concernenti gli *Open Data* e il riutilizzo dei dati pubblici, si veda il numero monografico di Informatica e Diritto, *Open Data e riuso dei dati pubblici*, 2011, n. 1-2.

107 Cfr. M. Orefice, *op. cit.*, p. 158. I soggetti in grado di effettuare un'efficace concentrazione delle informazioni sono rappresentati non solo da Google, Facebook o Microsoft, ma anche dai governi autoritari, così come dalle agenzie di sicurezza governative in missione antiterroristica. In questa direzione, si pongono, infatti, le numerose iniziative legislative moltiplicatesi dopo l'11 settembre 2001, data dell'attacco alle Torri gemelle di New York, e volte a contrastare il terrorismo internazionale quali, negli USA il *Patrioct Act* del 26 ottobre 2001 o, nel Regno Unito, l'*Anti-Terrorism, Crime and Security Act*, sempre del 2001, che possono interferire con la privacy dei cittadini. In particolare, negli USA, dopo l'11 settembre 2001, la *National Security Agency* (Nsa) ha sottolineato come, per scongiurare la minaccia terroristica, fosse indispensabile un'attività di sorveglianza continua applicando la tecnica del *data mining* ad ogni oggetto *online* utilizzato nella vita quotidiana. Solo nel 2015, con l'emanazione del *Freedom Act*, il Senato statunitense ha inteso limitare la sorveglianza indiscriminata della Nsa, anche se tale provvedimento è stato da molti avvertito come troppo blando e non in linea all'incessante crescita tecnologica. Nel contesto contemporaneo, segnato dalla minaccia terroristica, nonché da frequenti attacchi informatici, è particolarmente sentita la necessità di un contemperamento degli interessi coinvolti, come si evince, ad esempio, nel riferimento alla sicurezza nazionale e alla sicurezza pubblica contenuto all'art. 13 della Direttiva 95/46 e all'art. 23 del Regolamento UE 2016/679. Ci si trova, in tali casi, nell'ambito estremamente delicato dell'arduo bilanciamento tra la sicurezza dell'informazione e il rischio di un suo ipercontrollo e nella difficile conciliazione tra interessi pubblici e privati, cfr. S. Palanza, *op. cit.*, 14. Sul nesso e sul bilanciamento tra valori costituzionalmente tutelati quali la liberà di comunicazione, di informazione e la tutela della riservatezza personale in Internet, cfr. M. C. De Vivo, *Comunicare in Internet. Con che diritto?* in: "Informatica e Diritto", XXVI (2000), vol. IX, n. 2, pp. 125-158.

108 La *Sentiment analysis* utilizza tecniche di analisi testuale e altre tipologie di dati per estrarre e analizzare opinioni su prodotti, servizi e tendenze, cfr D. Talia, *op. cit.*, p. 101; cfr. M. Orefice, *op. cit.*, p. 25.

in discussione i più basilari princìpi democratici[109]. "Questi colossi sono oggi i maggiori intermediari di notizie e di informazioni, quindi di conoscenza, al punto che possono decidere cosa diffondere e cosa no, in quale forma e con quale viralità"[110]. La profilazione individuale, determinata dall'applicazione degli opportuni algoritmi – nei quali, va rilevato, la modifica di un unico parametro comporta risultati completamente diversi[111] - contribuisce, in tal modo, a selezionare contenuti determinanti per la formazione dell'opinione pubblica, da segnalare al singolo così come all'agenda politica[112]. Nella creazione di una *filter bubble*, volta a mostrare all'utente le informazioni che l'algoritmo ha calcolato per lui come potenziamente interessanti[113], si mostra tutta l'asimmetria tra chi offre il servizio informativo e il fruitore, aggravata dall'intrasparenza dei criteri posti alla base del funzionamento dell'algoritmo[114]. Ciò a dimostrazione dell'inesistenza di algoritmi neutrali, "di algoritmi che si limitano a riflettere la realtà, essi anzi propongono una loro versione fatta dalle formule classificanti, del peso attribuito ai singoli parametri inseriti, dalle procedure che determinano il risultato"[115]. Ovviamente, infatti, l'affermata simmetria comunicativa nel *Web* non implica un'effettiva parità nella condivisione della conoscenza, ma conferma, piuttosto, la disparità sociale tra chi detiene il potere informativo e coloro che non ne dispongono. Così, "nonostante l'enorme capacità che il mezzo digitale ha nel distribuire i dati e le informazioni a tutti, indistintamente e nello stesso istante, ognuno finisce per amplificare se stesso e non contribuisce all'amplificazione collettiva della critica e della protesta"[116]. Gli individui, come oggetti calcolabili, solo apparentemente condividono pensieri e azioni[117], riconoscendosi, con l'affidare la propria voce alla scrittura emotiva del *Web*[118], nei cosiddetti *sciami digitali*, raggruppamenti estemporanei che non aspirano e non riescono ad assumere la forma di soggetto socialmente strutturato. Di conseguenza, si può comprendere come la Rete, tramite l'impiego indiscriminato dei dati e l'invio di notizie ad indirizzi opportunamente selezionati, possa trasformarsi da spazio aperto ad ambito chiuso da precise corrispondenze, facendo sorgere gravi interrogativi sul piano della libertà di espressione e del pluralismo informativo[119]. Alla quantità di informazione a disposizione *online* corrisponde, inoltre, una maggiore quantità di strategie di disinformazione basate su notizie false (*fake news*)[120], per cui la qualità dell'informazione dipende, in definitiva, dalla capacità di critica e di discernimento del fruitore finale[121]. Al riguardo, va qui ricordata la scorciatoia mentale del "pregiudizio di conferma" per il quale, nella selezione delle informazioni rilevanti, ci si sente, in genere, maggiormente attratti da quelle che confermano le convinzioni soggettive di partenza: in questa breccia si inserisce la selezione contenutistica operata dall'algoritmo a suggerire cosa possa probabilmente destare l'interesse, in base a preferenze già espresse[122]: tale procedimento, come si può notare, stabilisce un doppio filtro informativo, determinato dall'azione congiunta della scelta algoritmica e del pregiudizio di conferma[123]. Il problema del pluralismo informativo oggi, oltre a ri-

109 Cfr. ivi, p. 158 e p. 182; cfr. anche A. Simoncini, S. Suweis, *op. cit.*, pp. 94 sgg.

110 M. Orefice, *op. cit.*, p. 182.

111 Cfr. A. C. Amato Mangiameli, *Algoritmi e big data*, cit., p. 109.

112 Cfr. M. Delmastro, A. Nicita, *op. cit.*, p. 91.

113 Cfr. A. C. Amato Mangiameli, *Algoritmi e big data*, cit., p. 109.

114 Cfr. *ibidem*.

115 D. Talia, *op. cit.*, p. 97.

116 Ivi, p. 11.

117 Cfr. ivi, p. 97.

118 Cfr. Z. Bauman, *Consuming Life*, Cambridge, 2007; trad. it., *Consumo, dunque sono*, Bari, 2010, p. 96; su questo tema, si veda anche B-C HAN, *Nello sciame. Visioni del digitale*, Roma, 2015.

119 Cfr. M. Delmastro, A. Nicita, *op. cit.*, p. 115.

120 Cfr. ad es. D. Talia, *op. cit.*, p. 13.

121 Cfr. M. Delmastro, A. Nicita, *op. cit.*, p. 93; l'Autorità di controllo per le garanzie nelle comunicazioni ha avviato un tavolo di monitoraggio sull'autoregolazione posta in essere dai motori di ricerca e dai *social network*, anticipando il lavoro avviato dalla Commissione Europea con l'istituzione del *High Level Group on Fake News and Online disinformation*, cfr. ivi, p. 135.

122 Cfr. ivi, p. 95.

123 Cfr. ivi, p. 97.

guardare la concreta possibilità di accesso alle piattaforme virtuali concerne e coinvolge, allora, direttamente la natura dell'algoritmo che opera come filtro dei contenuti[124]. L'algoritmo delinea "un pensiero cristallizzato, un procedimento capace di risolvere efficacemente un problema, di calcolare un risultato, attraverso un insieme di passi complementari"[125]: pertanto, nel massimizzare, attraverso l'elaborazione e l'analisi dei dati rinvenuti, l'incontro tra la domanda e l'offerta di informazioni, l'efficienza algoritmica rischia di emarginare processi e decisioni legati al reale significato delle cose per affermare una dimensione puramente misurabile[126]. "Il problema è che ciò che rende efficiente l'algoritmo di una piattaforma digitale, nello scambio di beni e servizi (...) è esattamente ciò che mina la natura reciproca della libertà di espressione e il pluralismo. La natura dell'algoritmo è, infatti, proprio quella di eliminare, dalla nostra selezione del mondo, ciò che non ci somiglia e ciò che non ci piace"[127]. Nell'impossibilità di sottrarsi completamente alla polarizzazione dell'informazione e all'esposizione selettiva delle notizie, "dobbiamo chiedere all'algoritmo, soprattutto a quello che governa le piattaforme digitali globali, di imparare ad essere plurale. E per farlo servono regole"[128].

Conclusioni

Si mostra, ancora una volta, tutta l'urgenza di un'efficace regolazione dei Big Data, e più in generale, delle informazioni personali circolanti *online*, ispirata ai valori costituzionalmente garantiti[129] e diretta alla tutela dell'individuo dall'impiego improprio delle tecnologie informatiche, evitando ogni possibile deresponsabilizzazione attribuita alla capacità interpretativa degli algoritmi utilizzati[130]. Questo, nella prospettiva di un'innovativa delineazione di modelli di cittadinanza digitale attiva, a fondamento di un'effettiva libertà nella costruzione dell'identità personale. Si può ben comprendere come, a monte, ciò implichi e comporti la previsione di una più equa redistribuzione del potere informativo in Rete, capace di sostenere inedite opportunità di relazione tra società civile e istituzioni. Si rendono indispensabili, in altri termini, norme *e* procedure prodotte sinergicamente dalla tecnica e dal diritto, espressione di un tecno-diritto in evoluzione[131], in grado di sostenere la capacità di critica e l'evento inatteso[132], scongiurando ciò che Rodotà descriveva efficacemente, mettendone in luce tutti i rischi per le libertà personali, come "dittatura dell'algoritmo", ad emblema di una società della spersonalizzazione[133]. Del resto, "che la storia conduca al regno dei diritti

124 Sul possibile utilizzo dell'algoritmo decisionale in una pronuncia giudiziaria e sui necessari limiti di tale impiego, si veda A. Simoncini, S. Suweis, *op. cit.*, pp. 96-102; A. C. Amato Mangiameli, *Algoritmi e big data*, cit., p. 115-16.

125 D. Talia, *op. cit.*, p. 98. Attualmente si stanno implementando innovativi paradigmi che permettano agli algoritmi di "apprendere", cioè, di gestire l'evento non previsto, cfr. *ibidem*.

126 Cfr. ivi, p. 120.

127 M. Delmastro, A. Nicita, *op. cit.*, p. 116.

128 Ivi, p. 117.

129 Cfr. A. Simoncini, S. Suweis, *op. cit.*, p. 103.

130 Cfr. S. Rodotà, *Il mondo nella rete*, cit., p. 39. Al riguardo, si veda il documento *Statement on Algorithmic Transparency and Accountability*, sulla trasparenza e responsabilità degli algoritmi, pubblicato il 12 gennaio 2017 dall'USACM, Associazione statunitense sulla meccanica computazionale, nonché la Risoluzione del Parlamento Europeo sulla robotica, del 16 febbraio 2017. Quest'ultima, al punto n. 10, mette in luce le possibilità che derivano dalla robotica nonché le tensioni e i possibili rischi di tale impiego da valutare considerando la sicurezza personale, la salute, la libertà, l'integrità e la dignità della persona; al punto n. 11 sottolinea le numerose implicazioni di carattere etico e la necessità di tratteggiare un quadro unitario di riferimento; al n. 12 afferma i criteri dell'autodereminazione, della trasparenza, della protezione e di non discriminazione dei dati personali. Tali principi dovrebbero essere garantiti anche dalla possibilità di indagare la logica posta alla base di ogni decisione presa con procedure dell'intelligenza artificiale, tale da avere un impatto rilevante sulla vita delle persone, cfr. www.europarl.europa.eu. Sui procedimenti di automazione decisionale, sulla possibile e conseguente erosione della responsabilità soggettiva, nonché sulle più rilevanti conseguenze giuridiche, si veda G. De Anna, *op. cit.*, pp. 125-42.

131 Cfr. A. C. Amato Mangiameli, *Algoritmi e big data*, cit., p. 119.

132 Cfr. M. Orefice, *op. cit.*, p. 133.

133 Cfr. S. Rodotà, *Il mondo nella rete*, cit., p. 37.

dell'uomo anziché al regno del Grande Fratello può essere oggetto solo di un impegno"[134].

Arianna Maceratini è ricercatrice in Filosofia del Diritto presso la Facoltà di Giurisprudenza dell'Università degli Studi di Macerata e professore aggregato di Informatica Giuridica presso il Corso di Classe di Scienze dei servizi giuridici dell'Università degli Studi di Macerata. Tra i suoi lavori, Procedura come norma. Riflessioni filosofico-giuridiche su Niklas Luhmann, *Torino, 2001,* Discorso e norma. Profilo filosofico-giuridico di Jürgen Habermas, *Torino, 2010;* La sfera pubblica dei media nella teoria del discorso di Jürgen Habermas, *in "Tigor: Rivista di scienze della comunicazione e di argomentazione giuridica" (2016);* Il rischio dell'assicurazione contro i pericoli. Complessità e contingenza nella teoria sistemica di Niklas Luhmann, *in "Tigor: Rivista di scienze della comunicazione e di argomentazione giuridica" (2017);* Trust and Power. Potere, fiducia, sistemi, *in "Tigor: Rivista di scienze della comunicazione e di argomentazione giuridica" (2018);* Retrotopia. L'utopia che guarda al passato, *in "Tigor: Rivista di scienze della comunicazione e di argomentazione giuridica" (2018).* Individui, spazi e confini nella modernità liquida di Zygmunt Bauman, *in "Tigor: Rivista di scienze della comunicazione e di argomentazione giuridica" (2019).*

arianna.maceratini@unimc.it

Opere consultate

134 N. Bobbio, *op. cit.*, p. 266.

A.C. Amato Mangiameli, *Informatica giuridica. Appunti e materiali ad uso di lezioni*, Torino, 2015.

- *Algoritmi e big data. Dalla carta sulla robotica*, in: "Rivista di filosofia del diritto", VIII (2019), n. 1, pp. 107-124.

A. Ballarini (a cura di), *Novecento del diritto*, Torino, 2019.

Z. Bauman, *Consuming Life*, Cambridge 2007; trad. it., *Consumo, dunque sono*, Bari, 2010.

N. Bobbio, *L'età dei diritti*, Torino, 1990.

M. Calvo, F. Ciotti, G. Roncaglia, M. A. Zela, *Internet 2004. Manuale per l'uso della Rete*, Roma-Bari, 2003.

F. Casi, *Big Data ed etica dei dati*, in: www.consultadibioetica.org.

G. De Anna, *Automi, responsabilità e diritto*, in: "Rivista di filosofia del diritto", VIII (2019), n. 1, pp. 125-142.

M. Delmastro, A. Nicita, *Big data. Come stanno cambiando il nostro mondo*, Bologna, 2019.

M.C. De Vivo, *Comunicare in Internet. Con che diritto?* in: "Informatica e Diritto", XXVI (2000), vol. IX, n. 2, , pp. 125-158.

- *Privacy: la legislazione, le imprese, la P. A. e la formazione in Italia. Intervista a Maria Concetta De Vivo*, del 16 dicembre 2013, in: http://www.alavie.it.

J. Drexl, *Economic efficiency versus democracy: on the potential role of competition policy in regulating digital markets in times of posttruth politics*, in: Max Plank Institute for Innovation and Competition Research, dicembre 2016, paper n. 16, pp. 1-28.

C. Faralli, *Introduzione*, in: Ballarini A. (a cura di), *Novecento del diritto*, Torino, 2019, pp. 1-8.

B-C Han, *Nello sciame. Visioni del digitale*, Roma, 2015.

M. Iasselli (a cura di), *Diritto e nuove tecnologie. Prontuario giuridico ed informatico*, Milano ,2016.

- *Privacy e nuove tecnologie*, in M. Iasselli (a cura di), *Diritto e nuove tecnologie. Prontuario giuridico ed informatico*, Milano, 2016, pp. 121-194.

M. Lindstrom, *Small Data: i piccoli indizi che svelano grandi trend*, Milano, 2016.

P. Moro, C. Sarra (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Milano, 2017.

L. Nosari, *Potenzialità e problematiche afferenti l'utilizzo dei Big Data in materia di diritti umani*, in: https://www.cyberlaws.it.

M. Orefice, *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, Canterano,2018.

S. Palanza, *Internet of things, big data e privacy: la triade del futuro*, in: IAI, Documenti Istituto Affari Internazionali, 2016.

G. Pascuzzi, *Il diritto dell'era digitale*, Bologna, 2016.

F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, 2016.

J. Rifkin, *The Age of Access: The new Culture of Hypercapitalism, Where All of Life is a Paid-for-Experience*, New York 2000, trad. it., *L'era dell'accesso*, Milano, 2001.

S. Rodotà, Discorso conclusivo della Ventiseiesima Conferenza Internazionale sulla protezione dei dati (Breslavia, 13-16 settembre 2004).

- *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2012.

C. Sarra, *Business Intelligence ed esigenze di tutela: criticità del c.d. Data Mining*, in: P. Moro, C. Sarra (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Milano, 2017, pp. 41-63.

F.A. Schreiber, L. Tanca, *Etica e big data, sette principi per proteggere i diritti umani*, in: https://www.agendadigitale.eu.

A. Simoncini, S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in: "Rivista di filosofia del diritto", VIII (2019), n. 1, pp. 87-106.

D. Talia, *La società calcolabile e i big data. Algoritmi e persone nel mondo digitale*, Catanzaro, 2018.

A.C. Zanuzzi, *Internet of things e privacy. Sicurezza e autodeterminazione informativa*, in: P. Moro, C. Sarra (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Milano, 2017, pp. 99-120.

Sitografia

https://www.agendadigitale.eu

http://www.alavie.it

https://www.cineca.it

www.consultadibioetica.org

https://www.cyberlaws.it

www.europarl.europa.eu

www.MyMarketing.net