

Autonomia e responsabilità nell'epoca delle *self-driving car*. Teorie etiche a confronto

NICOLA BUSTO*

SOMMARIO: 1. Il contesto. – 2. La posizione europea e gli spunti di cui alla precedente indagine. – 3. La posizione tedesca. – 4. Un potenziale elemento di contatto tra la posizione europea e quella tedesca. – 5. Una proposta di sintesi, la manopola etica. – 6. Considerazioni conclusive.

1. *Il contesto*

Il passaggio dalle azioni originariamente controllate dall'uomo a quelle controllate da sistemi tecnologici non è un fenomeno nuovo¹.

È quantomeno dalla fine dell'800², che vantaggi e svantaggi giuridici dell'introduzione di nuovi sistemi tecnologici vengono soppesati in ambito accademico.

In questo flusso plurisecolare di innovazione e dibattito, negli ultimi anni si è rinnovato l'interesse per gli sviluppi della cosiddetta "intelligenza

* Avvocato, attualmente contract manager nel settore consulenziale e tecnologico. Le opinioni espresse nel presente Articolo sono a titolo puramente personale.

¹ Basti fare riferimento alle recenti annotazioni di Floridi che fa risalire le origini della rivoluzione ICT a Blaise Pascal (1623-1662) ed alla invenzione, nel 1645, di una "macchina aritmetica", conosciuta come "Pascalina". Floridi la indica come il solo calcolatore meccanico in funzione nel XVII secolo, che ha dato la stura a tutte le future generazioni di macchine computazionali. Cfr. L. FLORIDI, *La quarta rivoluzione*, Capitolo 4, *Comprensione di sé: le quattro rivoluzioni*, pp. 103-106, Raffaello Cortina editore, 2017.

² Cfr. U. PAGALLO, *From Automation to Autonomous Systems: A Legal Phenomenology with Problems of Accountability*, par. 2.1, *Ancestors*, Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17), p. 17, "Scholars started examining the legal impact of automation, e.g. automatic vending machines, since the last decade of the 1800s. Think of Günther's *Das automatenrecht* (1892), Schels' *Der strafrechtliche Schutz des Automen* (1897), Schiller's *Rechtsverhältnisse des Automen and Ertel's *Der Automatenmissbrauch und seine Charakterisierung als Delikt*, both from 1898, up to Neumond's *Der Automat in 1899*". <https://www.ijcai.org/proceedings/2017/0003.pdf> (27/12/2018).*

artificiale”³ che – per usare le parole della Commissione Europea – «Come il motore a vapore o l’elettricità nel passato [...] sta trasformando il nostro mondo, la nostra società e la nostra industria. L’aumento della potenza di calcolo e della disponibilità dei dati e il progresso negli algoritmi hanno reso l’IA una delle tecnologie più strategiche del 21° secolo. La posta in gioco non potrebbe essere più alta. Il modo in cui ci relazioniamo all’IA determinerà il mondo in cui viviamo. Di fronte a un’acanita concorrenza mondiale, è necessario un solido quadro di riferimento europeo»⁴.

Al fine di costituire il menzionato «quadro di riferimento», gli studiosi paiono interessati, tra i molti temi, alla possibilità che l’intelligenza artificiale (unitamente alla robotica) possa trasformare i sistemi tecnologici oggi noti «[...] da oggetti meccanici, statici, recettivi, ripetitivi ed esecutivi, [...]» in «enti autonomi, mobili con funzioni generali e non solo specifiche, con capacità di apprendimento e adeguamento all’ambiente (anche senza il controllo di un operatore), in modo non sempre prevedibile, con capacità di cognizione analitica, comunicazione (riconoscimento della parola), espressione, emozioni o imitazioni delle emozioni umane nell’aspetto esteriore.[...]»⁵.

In altri termini, l’oggetto di uno dei principali dibattiti giuridici odierni è non tanto – come avvenuto in passato – l’automazione delle attività umane tramite sistemi tecnologici, quanto l’autonomia⁶ operativa e decisionale donata a quegli stessi sistemi dall’intelligenza artificiale.

³ Per un’introduzione al concetto di “intelligenza artificiale”, *ex multis*, cfr. N. BOLDRINI, “Cos’è l’Intelligenza Artificiale, perché tutti ne parlano e quali sono gli ambiti applicativi”, AI4Business.it, 9 giugno 2018, <https://www.ai4business.it/intelligenza-artificiale/intelligenza-artificiale-cose/> (27/12/2018).

⁴ Cfr. Comunicazione della commissione al Parlamento Europeo al Consiglio al Comitato economico e sociale europeo ed al Comitato delle regioni, Bruxelles 25/04/2018 COM (2018) 237 final, *L’intelligenza artificiale per l’Europa*, par. 1 “Introduzione – Accettare il cambiamento”, <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52018DC0237&from=IT> (27/12/2018)

⁵ Cfr. Presidenza del Consiglio dei Ministri, Comitato Nazionale per la bioetica e Comitato Nazionale per la biosicurezza le biotecnologie e le scienze della vita, *Sviluppi della robotica e della roboetica*, 17 luglio 2017, pp. 7 e 8. <http://presidenza.governo.it/biotecnologie/documenti/Robotica-misto%20CNB-CNBBSV-17lug17-IT.pdf> (27/12/2018).

⁶ Una discriminante che, ad avviso di chi scrive, deve essere posta a fondamento di ogni analisi di carattere etico-giuridico in quest’ambito, è quella riportata nel recente documento della Commissione Europea, intitolato *Statement on Artificial Intelligence, Robotics and ‘Autonomous’ Systems*. Come afferma lo *European Group on Ethics in science and new*

Autonomia e responsabilità nell'epoca delle self-driving car. Teorie etiche a confronto.

Numerosissime sono le iniziative in atto per la formulazione di principi etici per la governance della rivoluzione tecnologica dei robot “autonomi”. Industrie di settore, associazioni professionali, ONG, legislatori nazionali e continentali, sono tutti all’opera contemporaneamente. Il pericolo di una mancata armonizzazione di tutti questi interventi, che potrebbe portare ad una sorta di “*ethics shopping*”, è particolarmente sentito in ambito europeo. Esempio di tale disarmonia è un report pubblicato in Germania che sembra opporsi allo sviluppo delle self-driving car con livello di autonomia 5. Obiettivo di questo lavoro è evidenziare elementi di contatto e possibilità di avvicinamento tra la chiusura tedesca ed i quasi contestuali interventi di Parlamento e Commissione che paiono, muoversi in direzione diametralmente opposta.

Autonomy and responsibility in the age of self-driving cars. Comparing ethical theories.

There are several initiatives in place for the formulation of ethical principles aiming to the governance of the “autonomous” robots’ tech revolution. Industry, professional associations, NGO, national and continental legislators are all at work at the same time.

The lack of harmonization among said interventions could cause a sort of “ethics shopping”, a danger particularly perceived at European level. Example of said disharmony is a report published in Germany opposing the development of self-driving cars with a level of autonomy 5. The aim of this work is to highlight the elements of contact and the possibility of rapprochement between the German blocking approach and the almost simultaneous European Parliament and Commission interventions that seem to move in diametrically opposed direction.

Il cyberbullismo: le condotte tipiche e i soggetti coinvolti

SAMANTA STANCO*

SOMMARIO: 1. Introduzione. – 2. Le condotte tipiche. – 3. I soggetti coinvolti. – 4. Il cyberbullo. – 5. La vittima. – 6. Un confronto tra bullismo e cyberbullismo.

1. *Introduzione*

Uno degli ambiti dell'odio interpersonale che desta maggiore preoccupazione, e che tiene impegnati studiosi e giuristi a livello di politica sociale internazionale, è rappresentato dal cyberbullismo.

Il bullismo tradizionale, definito come l'adozione sistematica e ripetuta di un comportamento aggressivo contro determinati individui da parte di altri soggetti nell'ambito di un rapporto di poteri sbilanciato a favore del bullo, è un fenomeno diffuso in tutte le società sin dagli anni Settanta e coinvolge bambini e ragazzi in un'età particolarmente delicata. Gli effetti degli abusi in tal senso sui minori sono molto forti e possono ripercuotersi anche sul rendimento scolastico, nonché causare problemi di sonno, stress, dolori di stomaco, affaticamento, ansia, depressione, bassa autostima e sensazione di abbandono e di solitudine, spingendo addirittura la vittima al suicidio.

Il cyberbullismo, invece, è condotto soprattutto attraverso WhatsApp e i social network, oltre ad essere abbastanza diffuso su servizi e bacheche frequentati per lo più da adolescenti, e coinvolge una schiera di spettatori o partecipanti molto ampia, in quanto non è più limitato al solo gruppo di amici, ma è esteso anche a sconosciuti utenti del web; spesso, inoltre, non vi è percezione da parte del minore del reale impatto di ciò che egli commette davanti allo schermo. Dall'altro lato, per la vit-

* Cultore della materia "Informatica Giuridica" presso l'Università degli Studi di Milano.

tima risulta assai più complesso scappare dall'aggressione online e risalire all'identità dell'aggressore.

Le azioni nei confronti della vittima presentano sempre tre caratteristiche, che corrispondono ai fattori essenziali del cyberbullismo: l'intenzione di infliggere un danno, la presenza di uno squilibrio di potere tra le due parti e la ripetizione dei comportamenti lesivi, agevolata dalle tecnologie informatiche.

La rivoluzione tecnologica ha dunque mutato profondamente il quadro del bullismo: i nuovi strumenti elettronici a cui tutti hanno accesso hanno creato numerose opportunità di invasione della privacy nella vita di tutti i giorni, consentendo al contempo una minore esposizione del persecutore e una depersonalizzazione della vittima tali da rendere ancora più temibile la molestia.

2. *Le condotte tipiche*

Gli studiosi hanno più volte tentato di proporre una tassonomia del fenomeno del cyberbullismo. In particolare, nel 2006, Nancy Willard¹ ha individuato una serie di categorie specifiche che prendono in considerazione non gli strumenti utilizzati dal cyberbullo, bensì le fattispecie comportamentali da lui poste in essere. Da tale analisi sono emerse le seguenti condotte tipiche:

- *flaming*: con tale termine si indicano messaggi elettronici, violenti e volgari, mirati a suscitare “battaglie” verbali online tra due o più contendenti, per una durata temporale circoscritta all'attività online condivisa. È quanto accade, ad esempio, in caso di partecipazione ai videogiochi interattivi su Internet, dove i principianti, con il pretesto di errori inevitabilmente compiuti per via dell'inesperienza, vengono presi di mira con insulti e minacce e diventano oggetto di discussioni aggressive. Una lunga sequenza di messaggi di questo tipo (c.d. *flame war*) può talvolta precedere vere e proprie aggressioni nella vita reale;
- *harassment*: consiste nel ripetuto invio di messaggi scortesi, offensivi, insultanti e disturbanti attraverso e-mail, SMS, MMS, telefonate

¹ Cfr. N. WILLARD, direttrice del *Center for Safe and Responsible Internet Use*, in *Educator's Guide to Cyberbullying and Cyberthreats*, 2007.

Il cyberbullismo: le condotte tipiche e i soggetti coinvolti

Il fenomeno del bullismo è diventato oggi ancora più insidioso, potendo i suoi autori avvalersi dell'uso di strumenti tecnologici che non solo garantiscono una maggiore e più immediata invasività nella sfera personale delle vittime, ma che contribuiscono altresì ad eliminare qualsivoglia freno inibitore nei persecutori. Il presente saggio analizza alcuni aspetti peculiari del fenomeno, quali le condotte tipiche, la figura del bullo e della vittima e le differenze tra cyberbullismo e bullismo tradizionale.

Il cyberbullismo: le condotte tipiche e i soggetti coinvolti

Bullying is becoming more and more insidious among today's youth, due to the use of new technologies, that offer an easy way to harass other people feeling anonymous. This paper discusses general concepts within the area, such as types of cyberbullying, the role of the bully and of the victim, differences between cyberbullying and traditional bullying.

Internet e l'epoca delle Costituzioni capillari: il ruolo del costituzionalismo nella società digitale

ANDREA VENANZONI*

SOMMARIO: 1. L'epoca delle Costituzioni capillari. – 2. Internet tra paradigma libertario e istituzioni totali. – 3. Soggettività giuridiche e garanzie dei diritti nel “medioevo digitale”: il valore costituzionale della fiducia.

1. *L'epoca delle Costituzioni capillari*

L'espansione virale delle nuove tecnologie e le sempre più elevate caratteristiche performative di Internet stanno incidendo in maniera organica sui fenomeni di globalizzazione, determinando quella che per riprendere il titolo di un recente saggio di Richard Baldwin potremmo definire *grande convergenza*¹.

Una convergenza cioè tra finanziarizzazione dei moduli di progresso economico, sviluppo in rete della società mediante network e mediante connessioni aperte capaci di inglobare i Paesi in via di sviluppo in una ragnatela mercatoria: ne nascono paradigmi del tutto nuovi che incidono sulla caratterizzazione stessa delle regole giuridiche e sulla dimensione politica nonché sulle posizioni garantistiche di libertà individuali e collettive fino ad oggi fulcro delle Costituzioni originate dalle rivoluzioni liberal-democratiche.

* Dottorando di ricerca in Diritto Pubblico e Costituzionale, Dipartimento di Giurisprudenza - Università degli studi “Roma Tre”.

¹ R. BALDWIN, *La grande convergenza. Tecnologia informatica, Web e nuova globalizzazione*, il Mulino, Bologna, 2018. Nel cuore della nuova globalizzazione, è la tesi che muove il saggio di Baldwin, a differenza di quanto avvenuto in precedenza, network privati transnazionali e gruppi industriali cessano il percorso di agglomerazione territoriale industrializzata e iniziano processi di costruzione industriale in Paesi in via di sviluppo, ove grazie ai network informatici gestiscono i loro meccanismi di produzione come se non vi fosse effettivo divario territoriale tra sede-madre del network e sue ramificazioni.

Oggi, si ritiene², siamo in presenza di una quarta rivoluzione industriale, connessa a sviluppo ed espansione delle tecnologie informatiche: essa è un processo di produzione continua di informazioni e di loro scambio, basata su mercati accelerati e su dimensioni sociali del tutto modificate, in grado di alterare la percezione spaziale stessa³.

La socialità diventa una socialità digitale, si aprono sempre crescenti settori di mercato per la compravendita dei dati, la politica anela a nuove dimensioni rappresentative, prendendo atto della obsolescenza dei meccanismi parlamentari risalenti ormai al XIX secolo, e parlando sempre più insistentemente di democrazia digitale.

Soprattutto, nuove attorialità giuridiche sembrano emergere e Paesi di tradizione giuridica, culturale e sociale lontana da quella occidentale, come India e Cina, si sono al pari prepotentemente incistati nel discorso politico-economico globale.

Come in ogni rivoluzione che si rispetti, si registra una rottura; e da questa rottura originano frammenti di un mosaico complesso che devono essere tenuti insieme per evitare che i diritti fondamentali della persona e delle formazioni sociali possano decadere o sdilinquirsi.

Nel cuore di questa rottura si deve aprire una riflessione sul ruolo della scienza costituzionalistica in una società reticolare globale in cui le dimensioni spaziali e temporali differiscono radicalmente rispetto a quelle attorno cui la scienza costituzionalistica liberal-democratica si è storicamente formata; bisogna chiedersi quali nuovi scopi debba darsi una Costituzione e come essa possa preservare la distinzione tra poteri, garantendo la libertà individuale e dei gruppi e i diritti fondamentali nel bilanciamento democratico, continuando a promuovere diritti sociali, civili, in uno spazio virtualmente infinito e in cui la sovranità singolo-nazionale finisce per assumere connotazioni del tutto minoritarie rispetto alla arena globale.

Per focalizzare meglio il problema, bisogna chiedersi in primo luogo cosa nella concreta esperienza giuridica sia chiamata a fare una Costitu-

² Cfr. L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina, Milano, 2017. Sottolinea M. CASTELLS, *La nascita della società in rete*, EGEA, Milano, 2014, pp. 41 e ss. come si possa parlare a tutti gli effetti di rivoluzione determinata in punta di cambiamenti nella socialità, una effettiva micro-ingegneria nutrita da tecnologia informatica e comunicazione digitale.

³ L. FLORIDI, *La quarta rivoluzione*, op. cit., p. 55

Internet e l'epoca delle Costituzioni capillari: il ruolo del costituzionalismo nella società digitale

Il saggio investiga l'evoluzione del discorso costituzionale e dei relativi formanti, alla luce della emersione di Costituzioni civili, patrocinate in primo luogo dalla evoluzione tecnologica, dalla accelerazione dei dispositivi di comunicazione, dalla globalizzazione e dalla embricazione tra sfera privata e poteri pubblici. Una particolare attenzione viene dedicata alla net neutrality, sia nella sua prospettiva tecnica e regolatoria sia nella sua caratteristica costituzionale, e altrettanta attenzione viene dedicata alla ricerca di nuove garanzie costituzionali per preservare le libertà irrinunciabili del singolo.

Internet e l'epoca delle Costituzioni capillari: il ruolo del costituzionalismo nella società digitale

The essay investigates the evolution of the constitutional narrative and the basis of the connected topics, under the light of the rising civil Constitutions, built by the technological developments, by the high-speedy communication devices, by the globalization and the interlace between private and public powers. A particular attention is paid to net neutrality, both in its technical and regulatory perspective and in its constitutional characteristics, and the same amount of attention is paid to the research of new constitutional guarantees to preserve the fundamental rights and freedom.

La Pubblica Amministrazione nell'era delle ICT: sportello digitale unico e intelligenza artificiale al servizio della trasparenza e dei cittadini?*

DIANA-URANIA GALETTA **

SOMMARIO: 1. Buona amministrazione e tecnologie dell'informazione e della comunicazione: note introduttive. – 2. Competenze digitali e *digital divide*: scenari attuali e sfide aperte per la Pubblica Amministrazione 4.0. – 3. Le sfide poste dalle nuove tecnologie dal punto di vista dell'organizzazione e dell'attività amministrativa. – 4. *Open Government* e trasparenza: prospettive e sviluppi potenziali nel quadro tecnologico attuale. – 4.1. Trasparenza, partecipazione e *Open Government*. – 4.2. Disponibilità di informazioni e trasparenza: sinonimi o contrari?. – 4.3. Trasparenza e Intelligenza Artificiale: la trasparenza c.d. assistita e gli agenti conversazionali come strumenti di supporto per la Pubblica Amministrazione 4.0? – 5. Le sfide per l'Amministrazione Pubblica 4.0: osservazioni conclusive.

1. *Buona amministrazione e tecnologie dell'informazione e della comunicazione: note introduttive*

Negli ultimi decenni si è parlato molto di buona amministrazione e del legame, o delle differenze esistenti, tra i concetti di «buon governo» e quello di «buona amministrazione»¹.

Tuttavia nel contesto dell'Unione europea, sin dall'adozione della Carta dei diritti fondamentali dell'Unione europea, la buona ammini-

* Ringrazio il mio collega e amico Juan Gustavo CORVALÁN, Vice Procuratore generale per il contenzioso amministrativo e fiscale della Procura della Città di Buenos e Direttore del Laboratorio di Intelligenza Artificiale dell'Università di Buenos Aires (<https://liaa.dc.uba.ar/es/inicio/>). Molte delle riflessioni contenute in questo scritto sono infatti il risultato delle nostre interessantissime discussioni su questi temi e del mio soggiorno all'Università di Buenos Aires, nel novembre 2017.

** Professore Ordinario di Diritto Amministrativo e Coordinatore del Dottorato di ricerca in Diritto Pubblico, Internazionale ed Europeo presso l'Università degli Studi di Milano.

¹ Cfr. A. MOSCARIELLO, «El principio de la buena Administración», «El Derecho», Serie Especial Administrativo, 28/02/2013; P. SPANO TARDIVO, «El principio de transparencia de la gestión pública in el marco de la teoría del buen gobierno y la buena administración», «Revista Digital de la Asociación Argentina de Derecho Administrativo», 2016/1, pp. 226 ss.

strazione si caratterizza come un nuovo diritto fondamentale della persona²: Il diritto a una buona amministrazione, così come è scritto e dettagliato nell'articolo 41 di detta Carta³.

Si tratta di un diritto e non solamente di un principio guida dell'azione amministrativa. Ed è un diritto che, in sostanza, implica che il cittadino debba partecipare ed essere informato sulle questioni dell'amministrazione pubblica che lo riguardano. La nozione giuridica coincide, quindi, con quell'idea filosofica secondo cui una buona amministrazione pubblica è un'amministrazione che adempie alle funzioni che le sono proprie nel contesto di una democrazia, che è al servizio dei cittadini, che svolge il proprio lavoro in maniera razionale, giustificando le proprie azioni ed orientandosi continuamente all'interesse generale⁴. E si tratta di un interesse generale che – come è stato ben osservato – «nello stato di diritto sociale e democratico risiede nel miglioramento permanente e integrale delle condizioni di vita delle persone»⁵.

In questo senso, è convinzione di chi scrive che la rivoluzione legata all'utilizzo delle più moderne tecnologie dell'informazione e della comunicazione e all'uso dell'Intelligenza Artificiale, potrà/potrebbe aiutare molto a realizzare un'idea di buona amministrazione ancorata nella centralità della persona⁶.

Vediamo come e perché.

² Cfr. D.U. GALETTA, "Il diritto ad una buona amministrazione europea come fonte di essenziali garanzie procedurali nei confronti della Pubblica Amministrazione", «Rivista italiana di diritto pubblico comunitario», 2005/3, pp. 819 ss.

³ Sul che si rinvia, per tutti, a D.U. GALETTA, B. GRZESZICK, "Kommentar zu Art. 41 Grundrechtecharta", K. STERN/M. SACHS (a cura di), *Europäische Grundrechtecharta. Kölner Gemeinschafts-Kommentar*, Köln, 2016 (2^a ed.), pp. 618 ss.

⁴ Cfr. J. RODRÍGUEZ-ARANA, "La buena administración como principio y como derecho fundamental in Europa", «Derecho y Ciencias Sociales», N° 6, 2013, pp. 23 ss. (p. 26), reperibile anche in <https://dialnet.unirioja.es/descarga/articulo/5167578.pdf>.

⁵ J. RODRÍGUEZ-ARANA, *La buena administración* cit., p. 26 (la traduzione è mia). Cfr. Anche il contributo fondamentale di O. Höffe, *Gerechtigkeit als Tausch? Zum politischen Projekt der Moderne*, Baden-Baden, 1991, pubblicato nella serie "Würzburger Vorträge zur Rechtsphilosophie, Rechtslehre und Rechtssoziologie" (vol. 13).

⁶ «In este sentido, no podemos dejar de subrayar insistentemente la centralidad de la persona para la buena Administración pública. Efectivamente, el ser humano, con el cúmulo de circunstancias que lo acompañan in su entorno social, es el auténtico sujeto de los derechos y libertades. A ese hombre, a esa mujer, con su determinada edad, su grado de cultura y de formación, mayor o menor, con su procedencia concreta y sus intereses particulares, propios, legítimos, es a quien la Administración pública sirve para que se pueda desarrollar in libertad solidaria». J. RODRÍGUEZ-ARANA, *La buena administración* cit., p. 27.

La Pubblica Amministrazione nell'era delle ICT: sportello digitale unico e intelligenza artificiale al servizio della trasparenza e dei cittadini?

La rivoluzione legata all'utilizzo delle più moderne tecnologie dell'informazione e della comunicazione (ICT) e all'uso dell'Intelligenza Artificiale (AI) è ricollegata all'obiettivo di realizzare la c.d. buona amministrazione ed ancorata alla centralità della persona e dei suoi diritti. L'obiettivo è infatti di ridurre e certamente di non accrescere, attraverso il loro utilizzo, le attuali disuguaglianze presenti nella società, garantendo uno sviluppo sostenibile e inclusivo.

La Pubblica Amministrazione nell'era delle ICT: sportello digitale unico e intelligenza artificiale al servizio della trasparenza e dei cittadini?

The revolution connected to the use of the most modern Information and Communication Technologies (ICT) and the use of Artificial Intelligence (AI) is linked to the goal of achieving the so called good administration and anchored to the centrality of the person and his rights. The goal is, indeed, to reduce and certainly not to increase, through their use, the current inequalities in society, ensuring a sustainable and inclusive development.

Big data e People Analytics: nuove sfide e opportunità per liberare valore

ILENIA MARIA ALAGNA*

SOMMARIO: 1. I *Big Data* quali protagonisti della rivoluzione digitale. – 2. Il rapporto tra *Big data* e lavoro: la “*workforce analytics*”. – 3. I *Big Data* e la disciplina in tema di protezione dei dati personali. – 4. Le attività di trattamento dei dati personali all’interno dei contesti lavorativi. – 5. Conclusioni.

1. *I Big Data quali protagonisti della rivoluzione digitale*

La società «post-industriale» di cui facciamo parte può essere anche definita come «società dell’accesso» in virtù della crescente digitalizzazione dell’informazione e della possibilità di fruire di una grande quantità di dati attraverso l’ausilio delle nuove tecnologie. Queste ultime non rappresentano solo la fonte dei dati, ma anche il fattore abilitante per la loro analisi: si rende in tal modo possibile, da un lato, il trattamento simultaneo di innumerevoli dati e, dall’altro, l’estrazione di una mole di informazioni da esse. Tale è il c.d. fenomeno dei “*Big Data*”. Con tale espressione si intende un insieme di dati estremamente esteso in termini di volume, velocità e varietà da richiedere tecnologie innovative e specifici metodi analitici per l’estrazione di valore.

Nel corso degli anni si è ulteriormente arricchito il modello che, oltre alle tre V descritte in precedenza, aggiunge le caratteristiche di veridicità e variabilità. Mentre il primo termine fa riferimento alla qualità dei

* Ilenia Maria Alagna, Avvocato e consulente legale in materia di tutela e sicurezza dei dati personali, privacy digitale e diritto delle nuove tecnologie. Si è laureata in Giurisprudenza all’Università di Ferrara ed ha conseguito il Master in “Diritto delle Nuove tecnologie e Informatica Giuridica” presso il CIRSIFID di Bologna ed il Master in “Privacy Officer” presso Asso Dpo. È Fellow dell’Istituto Italiano Privacy e la valorizzazione dei dati e Cultrice della materia in “Informatica Giuridica” presso l’Università degli Studi di Milano. È autrice di studi e articoli giuridici in tema di privacy e diritto di Internet.

dati e alla loro affidabilità, il secondo esprime la mutevolezza del significato o dell'interpretazione di un dato a seconda del contesto in cui lo stesso viene raccolto e analizzato. I *Big Data* sono dunque dati eterogenei per fonte e formato, caratterizzati da elevati volumi e da elevata velocità di generazione-acquisizione, che devono garantire la descrizione di dati veritieri e dal significato contestualizzabile¹.

L'Organizzazione per la cooperazione e per lo sviluppo economico, OECD, ha affermato che «l'analisi dei *Big Data*, sempre più in tempo reale, sta guidando la creazione di conoscenza e valore all'interno della società; incoraggiando la creazione di nuovi prodotti, processi e mercati; incentivando la nascita di modelli di business completamente nuovi; trasformando la maggior parte dei settori nei paesi dell'OECD e nelle economie partner; e con ciò rafforzando la competitività economica e la crescita della produttività». Si tratta in particolare della c.d. "innovazione basata sui dati" (*data-driven innovation*)².

Sulla base di quanto sopra affermato i *Big Data* rappresentano una fonte inestimabile di valore ma limitarsi a raccogliere i dati, pur sfruttando le migliori tecnologie disponibili sul mercato, non garantisce alle organizzazioni di possedere informazioni dalle quali estrarre conoscenza. Parlare di dati, informazioni e conoscenza vuol dire porre in relazione fra loro aspetti differenti.

Per definizione un dato è una rappresentazione codificata di un'entità, di un fenomeno, di una transazione o di un avvenimento. L'informazione è il risultato di un processo di analisi del dato, spesso rileva solo per colui che opera nel dominio di generazione del dato. La conoscenza si ottiene quando una persona utilizza le informazioni per prendere decisioni e realizzare azioni, quando le informazioni vengono utilizzate per essere messe "in pratica".

Per attuare tale processo, e far sì che i *Big Data* possano essere trasformati in informazioni da utilizzare nei processi aziendali costruendo conoscenza per migliorare le performance, sono necessari strumenti di *Analytics*. È doveroso considerare un ulteriore V nel momento in cui si

¹ Cfr. A. PIVA, I. GUINDANI, "Il Contesto di riferimento - Parte 1", *Big Data Analytics, Leve di progettazione sfide e opportunità, ambiti di applicazione*, «IlSole24 ore», 2017, p. 14.

² Cfr. "Data-Driven Innovation: Big Data for Growth and Well-Being", OECD Publishing, 2015.

Big data e People Analytics: nuove sfide e opportunità per liberare valore

Nell'attuale economia della conoscenza si presta sempre più attenzione alla raccolta e all'analisi dei dati dal momento in cui, in ogni contesto produttivo e sociale, la quantità di essi, è soggetta ad incrementare rendendo inadatte le tradizionali tecniche di analisi. In tal senso le nuove tecnologie rappresentano un valido strumento, rendendo possibile al contempo l'elaborazione dei dati e l'estrazione delle informazioni da essi provenienti attraverso il fenomeno dei c.d. "Big Data". Gli operatori del mercato digitale riconoscono a tale fenomeno un ruolo centrale, riscontrabile in investimenti economici significativi in molteplici settori aventi la finalità di gestire le politiche aziendali, quelle organizzative nonché gli aspetti legati alle risorse umane.

Big data e People Analytics: nuove sfide e opportunità per liberare valore

In the current knowledge economy, more and more attention is paid to the collection and analysis of the given data, which, in any productive and social context, the quantity of them is subject to increasing rendering traditional analytical techniques unsuitable. In this sense, new technologies are a valid tool, making it possible at the same time for the processing of data and the extraction of information coming from them through the phenomenon of c.d. "Big Data". Operators of the digital market recognise this phenomenon as increasingly bearing a central role that can be found in significant economic investments in many sectors with the aim to manage company's policies, organizational policies and aspects related to human resources.

La verifica preliminare dell'autorità di controllo su disposizioni legislative o regolamentari

JEAN LOUIS A BECCARA*

SOMMARIO: 1. Inquadramento. – 2. La riconducibilità alle sole ipotesi di “rischio elevato”. – 3. Verso una soluzione più “estrema”. – 4. Conclusioni.

1. *Inquadramento*

Ai sensi dell'art. 36, paragrafo 4, del Regolamento UE 2016/679 (di seguito, il GDPR) «gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento».

Tale disposizione, se non altro per una questione di parità di rango nelle fonti del diritto, dovrebbe potersi facilmente estendere anche alle leggi regionali e delle Province autonome, nonché ai relativi atti regolamentari¹. Ciò implica che la problematica relativa all'effettiva portata dell'art. 36.4 del GDPR, diretta a stabilire quando sia necessario consultare preventivamente l'Autorità Garante nella stesura di un atto normativo, non possa che assumere ulteriore spessore.

Dal momento che la suddetta disposizione europea non stabilisce un termine iniziale, ovvero una condizione o un presupposto da cui sca-

* Avvocato. Già responsabile dell'Ufficio legale di Cassa Centrale Banca S.p.a., è oggi Direttore dell'Ufficio “Organizzazione e gestione della privacy” della Provincia autonoma di Trento. È autore del volume “La privacy nel pubblico”, nonché di ulteriori pubblicazioni su riviste scientifiche e specialistiche.

¹ Si pensi, a tale proposito, al regolamento per il trattamento dei dati “sensibili” e “giudiziari”, un tempo previsto all'art. 20 ed oggi individuato all'art. 2-*sexies* del D. Lgs. 196/2003; regolamento che, per l'appunto, deve ora disciplinare anche le misure appropriate e specifiche per mitigare i rischi. Pertanto, potrebbe essere ancora necessaria l'approvazione di tale atto normativo da parte del Garante (come al previgente art. 20 del D. Lgs. 196/2003), nei termini di seguito descritti.

turisca l'obbligo di consultazione, un'interpretazione prettamente letterale dell'art. 36.4 produrrebbe, quale immediata conseguenza, il dovere del Parlamento, del Governo, delle Regioni e degli organi legislativi degli enti locali di sottoporre al Garante ogni atto normativo in corso di elaborazione. Soluzione, questa, che non solo potrebbe creare una notevole *impasse* all'attività della stessa Autorità, ma che appare – almeno *prima facie* – aberrante, priva di un fondamento logico, oltre che incoerente rispetto alla presumibile *ratio legis*.

2. *La riconducibilità alle sole ipotesi di "rischio elevato"*

Una lettura sistematicamente orientata vedrebbe nella collocazione della disposizione nell'ambito della valutazione d'impatto (*data privacy impact assessment*) un elemento da non sottovalutare nell'individuazione dell'esatto ambito applicativo della norma. Valutazione d'impatto che, sostanzialmente, ha sostituito tanto il c.d. "*prior checking*" di cui all'art. 17, quanto la notifica preliminare di cui all'art. 37 del previgente Codice (D. Lgs. 196/2003), entrambi concernenti trattamenti che avessero presentato un certo grado di rischio.

Ebbene, se la DPIA è una misura² diretta alla mitigazione di un rischio notevole (per i diritti e le libertà degli interessati) insito nel trattamento effettuato e tale misura comporta un intervento del Garante soltanto eventuale e nel limite in cui tale rischio permanga a un livello elevato (nonostante³ le misure tecniche ed organizzative adottate per attenuarlo), lo scopo della disposizione di cui all'art. 36.4 parrebbe quello di obbligare a ottenere un intervento del Garante non più eventuale e in fase successiva, bensì preventivamente, ma pur sempre sulla base degli stessi presupposti di cui all'art. 36 del GDPR.

Ciò implica che la consultazione preventiva dovrebbe concernere esclusivamente i progetti normativi che presentassero, anche alla luce delle Linee Guida del Gruppo di Lavoro Art 29 sulla DPIA (WP 248), una certa connotazione di rischio⁴.

² Valutazione da effettuare, comunque, prima di iniziare il trattamento.

³ Tale preposizione, infatti, sarebbe dovuta essere utilizzata al posto dell'inciso, poco felice, "in assenza" (tant'è, che nel WP 248 ci si riferisce alla presenza di "rischi residui" elevati).

⁴ Si tenga altresì presente, per la legislazione regionale, l'ulteriore limite fissato dalla Corte Costituzionale nella nota sentenza n. 271/2005.

La verifica preliminare dell'autorità di controllo su disposizioni legislative o regolamentari

Il paper esamina la disposizione di cui all'art. 36.4 del GDPR e, in particolare, l'effettiva portata applicativa nei confronti della Pubblica Amministrazione, in assenza di precisazioni normative a riguardo. Interrogativo, questo, di notevole interesse per gli Enti pubblici territoriali che, si rammenta, effettuano i trattamenti in base al combinato disposto degli artt. 6.1, lett. e) e 6.3 del GDPR, nonché dell'art. 2-ter, comma 1, del D. Lgs. 196/2003. Presupposto fondamentale della presente dissertazione è che per sottoporre all'Autorità di controllo un progetto di legge, non si possa prescindere dall'aver previamente effettuato una DPIA. Per esaminare un disegno normativo, infatti, è necessario descrivere il trattamento e, in particolare, le finalità, i dati in oggetto, nonché le misure di sicurezza adottate (sulla base della, propedeutica, individuazione dei rischi). Come risulterà nel corso della trattazione, per un corretto inquadramento della problematica, dovrebbe tenersi debitamente conto anche dell'attuazione, recentemente avvenuta a livello nazionale con il D. Lgs. 101/2018, della disposizione di cui all'art. 36.5 dello stesso GDPR. In conclusione, si tratterà di comprendere se, nonostante l'assenza di specifici presupposti che circoscrivano l'ambito applicativo dell'obbligo di consultazione del Garante, tale coinvolgimento si renda necessario soltanto in situazioni che presentino un "rischio elevato" o, addirittura, "particolarmente elevato".

The preliminary verification by the Control Authority in relation to legislative and regulatory provisions

The paper examines the provision set out in article 36.4 of the GDPR and, in particular, the actual applicability of the same vis-à-vis the Public Administration, since the law does not contain specific provisions in this regard. This question is of considerable interest for the territorial public bodies which, it is recalled, carry out the treatments on the basis of the combined provisions of the articles 6.1, letter e) and 6.3 of the GDPR, as well as of the article 2-ter, subsection 1, of Legislative Decree no. 196/2003. A fundamental prerequisite of the present dissertation is that in order to submit a draft law to the Control Authority, it is necessary to have previously carried out a DPIA. In fact, to examine a legislative proposal, it is necessary to describe the treatment and, in particular, the purposes, the data in subject, as well as the security measures adopted (on the basis of the preliminary identification of the risks). As will it be seen in the

course of the discussion, for a correct classification of the problem, it should be duly keep in mind also the implementation of the provision contained in article 36.5 of the same GDPR, recently occurred at national level with the Legislative Decree no. 101/2018.

In conclusion, it will be necessary to understand whether, despite the absence of specific conditions that circumscribe the applicative scope of the obligation of consultation of the Guarantor, such involvement is necessary only in situations that present a “high risk” or, even, a “particularly high risk”.

La protezione dei dati personali nel cloud: dati e rischi dal punto di vista dell'azienda

MICHELA CERULLO^{*}, EDOARDO FACCHINI^{**},
ALESSANDRA LUCCHINI^{***}, PAOLO PINTO^{****}

SOMMARIO: 1. Premesse: il cloud in generale – modelli di servizio, – 2. Cenni sul Regolamento Europeo n. 679/2016 sulla protezione dei dati personali. – 3. Rapporti tra titolare e fornitore: nomina a responsabile del trattamento - Il contratto di servizio. – 4. Il tipo di dati ed i rischi collegati. – 5. Conclusioni.

1. *Premesse: il cloud in generale – modelli di servizio*

Il cloud è uno spazio di archiviazione personale, accessibile da chiunque, in qualunque momento e da qualsiasi luogo mediante una

* Si è laureata in Giurisprudenza presso l'Università Cattolica del Sacro Cuore di Milano, dopo aver trascorso un periodo in qualità di Visiting Scholar presso la Yale University (USA). Ha svolto uno Stage Curriculare presso lo Studio Legale Clifford Chance di Milano. Ha, frequentato un corso di perfezionamento in "Fashion Law" e in "Data Privacy e Data Governance" presso l'Università degli Studi di Milano, nonché il "General Course on Intellectual Property" presso l'Organizzazione Mondiale della Proprietà Intellettuale" (Svizzera) e "EUTM in a Nutshell", presso l'Ufficio dell'Unione Europea sulla Proprietà Intellettuale (Spagna). Praticante Avvocato.

** Ingegnere delle Telecomunicazioni con MBA. Esperienza decennale in ambito networking lato prevendita e formazione tecnica prima presso vendor multinazionali poi con attività in proprio. Libero professionista collabora attualmente con diverse realtà in ambito formazione e privacy.

*** Avvocato Cassazionista del foro di Milano. Da anni si occupa di tutela di protezione e trattamento dei dati personali sia in ambito pubblico sia privato. Esercita l'attività di DPO per una primaria compagnia di assicurazione. Fornisce altresì attività di consulenza per intermediari assicurativi, compagnie e aziende private.

**** Laureato in Ingegneria Aeronautica presso l'Università Federico II di Napoli, vi ha successivamente conseguito il Dottorato in Trasporti occupandosi di analisi dei dati e Intelligenza Artificiale e svolgendo successivamente per 4 anni attività di Ricerca Accademica presso il Dipartimento di Progettazione e Gestione Industriale. Libero Professionista, collabora attualmente con diverse Aziende in tema di Data Driven Marketing e Privacy Compliance.

connessione Internet. Con il termine cloud si fa riferimento al cloud storage e al cloud computing. Il primo, sincronizza tutti i propri file preferiti in un unico posto, con il vantaggio di poter scaricare, modificare, cancellare o aggiornare i medesimi in un momento successivo senza aver bisogno dell'ausilio di un hard disk esterno e di una penna USB. Il cloud storage permette, altresì, di realizzare copie di backup nonché condividere i file con terzi senza un limite di tempo¹.

Il secondo, permette di archiviare, elaborare o trasmettere dati on demand attraverso l'uso della rete Internet. Ciò significa che mediante il cloud computing è possibile utilizzare risorse le cui caratteristiche non sono note all'utilizzatore.

Il cloud può distinguersi anche in base a infrastruttura, capacità elaborativa e software.

Infine, con riferimento alle proprietà delle risorse utilizzate dal cloud, si distingue in pubblico, privato o ibrido.

Da questa classificazione si capisce che il termine cloud ingloba una grande varietà di soluzioni. Sta all'Azienda, a seconda delle sue esigenze produttive, scegliere quella che soddisfa le sue necessità.

2. *Cenni sul nuovo Regolamento Europeo n. 679/2016 sulla protezione dei dati personali*

Con la locuzione dati personali «si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale»².

La vigilanza sul corretto utilizzo di questi dati è affidata al Garante per la protezione dei dati personali, intesa quale Autorità amministrativa indipendente. Quest'ultima è stata istituita a seguito dell'entrata in vigore della prima Legge sulla Privacy, L. 675 del 1996, in attuazione della

¹ Per maggiori dettagli sulla definizione di cloud e sulle sue classificazioni, <http://www.informaticapertutti.com>.

² Art. 4, n. 1), Regolamento UE n. 679/2016.

La protezione dei dati personali nel cloud: dati e rischi dal punto di vista dell'azienda

Il 25 Maggio 2018 è entrato in vigore il nuovo Regolamento Privacy n. 679/2016, relativo alla protezione dei dati personali. L'obiettivo di questo studio è quello di evidenziare le novità del nuovo Regolamento Europeo, nonché comprendere il modo in cui è possibile proteggere i dati personali nel Cloud, mediante un'analisi pratica di un contratto di servizi e dei diversi tipi di dati. Le risposte fornite evidenziano che, al fine di proteggere i dati personali, un'Azienda deve necessariamente, al momento della stipula del contratto, attenersi agli obblighi e alle garanzie che il contratto stesso richiede per evitare di incorrere nelle sanzioni previste dal presente Regolamento.

La protezione dei dati personali nel cloud: dati e rischi dal punto di vista dell'azienda

On May 25th 2018 the New Privacy Regulation n. 679/2016 came into force, concerning the protection of personal data. The objective of this study is to highlight the novelties of the New European Regulation, as well as to understand how it is possible to protect personal data in the Cloud, through a practical analysis of a service contract and the different types of data. The answers provided show that, in order to protect personal data, a Company must necessarily, at the time of signing the contract, comply with the obligations and guarantees that the contract requires to avoid incurring the sanctions provided for in this Regulation.

La blockchain: una lettura giuridica per uno sguardo verso il futuro

MICHELE CHIERICI*

SOMMARIO: 1. Premessa. – 2. Moneta, moneta elettronica e moneta virtuale. – 2.1. Struttura e qualificazione giuridica del bitcoin. – 2.2. La normativa antiriciclaggio e il problema delle monete virtuali. – 2.3. Pagamenti in cui una prestazione ha per oggetto bitcoin. – 2.4. La normativa comunitaria attuale. – 3. La blockchain applicata al settore immobiliare: pro e contro. – 4. SPID (Sistema Pubblico di Identità Digitale) e blockchain. – 5. Altre applicazioni della blockchain: gli *smart contracts*. – 6. Conclusioni.

1. *Premessa*

Una delle più grandi innovazioni tecnologiche future e presenti è senza dubbio rappresentata dalla crescita della struttura blockchain¹. Anche a livello giuridico ultimamente il legislatore, sia nazionale che internazionale², ha previsto una prima serie di norme volte a regolamentare alcuni aspetti inerenti le nuove tecnologie.

* Laureato in Giurisprudenza presso l'Università degli Studi di Parma, appassionato di nuove tecnologie e del loro impatto sul sistema giuridico, sia nei rapporti tra privati che nella sfera pubblica. Attualmente, e durante la stesura dell'elaborato, l'autore non ha, e non ha avuto, alcuna moneta virtuale tra le sue disponibilità.

¹ Cfr. R. FERRARI, *L'era del fintech: la rivoluzione digitale nei servizi finanziari*, Milano, Franco Angeli Editore, 2016 per il quale la blockchain può avere interessanti applicazioni sia nel mondo bancario che non.

² Tra tutti l'Associazione Bancaria Europea sta svolgendo attività di ricerca in materia di criptovalute, ma anche la Banca Centrale Europea si sta occupando della regolamentazione di alcuni aspetti soprattutto relativi alla moneta virtuale.

Questa nuova tecnologia sempre più dibattuta offre una moltitudine di vantaggi³ (e anche qualche svantaggio⁴) che non possono essere ignorati nel panorama attuale. Anche dal punto di vista giuridico introduce alcune interessanti varianti, ad esempio si pensi ai nuovi metodi di pagamento sicuri⁵, alla tenuta dei registri pubblici, a una rivoluzione del sistema di votazione (c.d. *e-voting*⁶) o all'introduzione degli *smart contracts*. In particolare il fenomeno blockchain ha avuto la sua espansione grazie alla creazione dei bitcoin, ovvero il motivo principale per il quale fu creata. Indubbiamente tuttavia, risulta più interessante la struttura che permette l'esistenza dei bitcoin piuttosto che i bitcoin stessi⁷.

³ Cfr. G. GASPARRI, "Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?", in «Diritto dell'informazione e dell'informatica», III, Milano, 2015, p. 415 data la sicurezza e allo stesso tempo la velocità che possono avere gli scambi di moneta virtuale, è prospettabile una applicazione nei micropagamenti e qualsiasi altro genere di transazione di modico valore, si potrebbe addirittura concepire una retribuzione settimanale e non mensile, oppure potrebbe essere utilizzata in ambito di *crowdfunding* per le migliaia di piccole donazioni. Essendo inoltre dotata di una certa sicurezza, potrebbe infine fungere da struttura anche per i pagamenti di grandi dimensioni, come l'acquisto di un immobile. Allo stesso tempo anche le transazioni che avvengono quotidianamente sulle piattaforme di *e-commerce* potrebbero essere supportate da questa tecnologia, quindi sia a favore dei commercianti, sia a favore dei consumatori.

⁴ Spesso si parla della grande capacità di calcolo richiesta dai *miners* nell'ambito delle loro operazioni, ciò comporta un enorme dispendio di energia per il funzionamento degli *hardware* che per 24 ore al giorno eseguono migliaia di calcoli ogni secondo. Un altro problema potrebbe essere localizzato nella sicurezza non tanto del sistema ma dei computer degli utenti che ben più facilmente potrebbero essere oggetto di attacchi hacker. Inoltre se una chiave privata viene persa, il proprietario contestualmente perde tutte le transazioni riferite alla chiave pubblica corrispondente. Così anche se un soggetto diverso dal proprietario si appropria della chiave, potrà effettuare transazioni irrevocabili una volta che queste verranno salvate nella blockchain.

⁵ Cfr. J. BONNEAU, A. MILLER, J. CLARK, A. NARAYANAN, J.A. KROLL, E.W. FELTEN, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", 2015, consultabile a <http://www.jbonneau.com/doc/BMCNK15-IEEEESP-bitcoin.pdf> (link attivo il 27/8/2018), 2015.

⁶ P. BOUCHER, "What if lockchain technology revolutionised voting?", 2016 consultabile a http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA%282016%29581918_EN.pdf (link attivo il 27/8/2018) la blockchain potrebbe incamerare i voti utili poi per il conteggio che sarà effettuato dall'autorità centrale. Già a partire da alcune simulazioni interne ai partiti e da un primo test effettuato in Estonia si è subito percepita la potenzialità di questo mezzo.

⁷ Cfr. R. ALI, J. BARRDEAR, R. CLEWS, J. SOUTHGATE, "The economic of digital currencies", «Bank Of England Quarterly Bulletin», 2014, p. 277 per i quali «The key

La blockchain: una lettura giuridica per uno sguardo verso il futuro

L'avvento della tecnologia blockchain porta inevitabilmente con sé nuove problematiche sia tecniche che giuridiche. Soffermandosi soprattutto su queste ultime, sono stati analizzati quattro settori di particolare interesse: le monete virtuali, il settore immobiliare, l'identità digitale e i contratti automatizzati. Per ogni categoria si riportano le questioni di maggior rilievo giuridico, ossia l'inquadramento giuridico delle valute virtuali e il pericolo del riciclaggio, l'assenza di un soggetto certificatore nelle transazioni immobiliari, la verifica dei dati personali delle identità digitali e la eccessiva rigidità dei contratti automatizzati.

Blockchain: a legal reading for a look into the future

The advent of blockchain technology inevitably brings with it new technical and legal problems. This paper analyze four sectors of particular interest: virtual currencies, real estate, digital identity and automated contracts. For each category are reported the most important legal issues, define a legal framework of virtual currencies and the money laundering problem, the absence of a certifying party in real estate transactions, the verification of personal data of digital identities and the excessive rigidity of automated contracts.

Il consenso dell'Interessato come condizione per l'offerta di un servizio - La sentenza della Corte di Cassazione 17278/2018

LUCREZIA FALCIAI*

SOMMARIO: 1. Il fatto. – 2. Le motivazioni della Corte di Cassazione. – 3. L'orientamento del Garante per la protezione dei dati personali e le Linee Guida del *Working Party* 29. – 4. Conclusioni.

1. *Il fatto*

Il Tribunale di Arezzo, con sentenza emessa il 29 aprile 2016, aveva accolto il ricorso proposto dalla società AdSpray S.r.l. contro il provvedimento del Garante per la protezione dei dati personali del 25 settembre 2014.

La società in questione era stata sanzionata in quanto, per consentire all'utente di fruire del servizio offerto tramite il proprio sito Internet, richiedeva un consenso al trattamento dei dati personali di quest'ultimo. In particolare, tra i trattamenti riportati nell'informativa privacy fornita agli interessati, veniva indicato che i dati in questione sarebbero stati utilizzati per inviare comunicazioni a contenuto commerciale.

Di conseguenza, in sostanza, la AdSpray S.r.l., subordinava la fruizione dei servizi offerti attraverso il proprio sito all'espressione di un unico generico consenso al trattamento di dati personali di colui che volesse usufruirne, utilizzando, poi, i dati raccolti per trattamenti ulteriori rispetto a quelli strettamente necessari a fornire il servizio.

Il Garante per la per la protezione dei dati personali, aveva ritenuto che il consenso così espresso non fosse liberamente prestato, stabilendo,

* Dottoressa in Giurisprudenza presso l'Università degli Studi di Milano. Già laureata in Scienze politiche - Istituzioni e relazioni internazionali presso l'Università Cattolica di Milano.

di conseguenza, l'illiceità del trattamento posto in essere dalla AdSpray S.r.l. e vietando alla società l'ulteriore trattamento dei dati raccolti.

Al contrario, il Tribunale di Arezzo, aveva ritenuto che il consenso dell'utente non potesse ritenersi non liberamente espresso, poiché la normativa in materia di protezione dei dati personali non individuava un obbligo per il gestore del sito di offrire comunque le proprie prestazioni a prescindere dal consenso al trattamento.

Inoltre, sempre secondo il Tribunale, non erano condivisibili le affermazioni del Garante per la protezione dei dati personali, il quale aveva sostenuto, in particolare, che il consenso non fosse prestato in conformità con l'articolo 23 del D.Lgs 196/2003 ("Codice Privacy") in quanto, come stabilito all'interno delle Linee guida in materia di attività promozionale e contrasto allo spam del 2013, «Il consenso del contraente per l'attività promozionale deve intendersi libero quando non è preimpostato e non risulta – anche solo implicitamente in via di fatto – obbligatorio per poter fruire del prodotto o servizio fornito dal titolare del trattamento» e che «non è libero il consenso prestato quando la società condiziona la registrazione al suo sito web da parte degli utenti e, conseguentemente, anche la fruizione dei suoi servizi, al rilascio del consenso al trattamento per la finalità promozionale»¹.

Il Tribunale di Arezzo ha giustificato la propria posizione sostenendo che le Linee guida citate dal Garante per la protezione dei dati personali costituivano un'integrazione di quanto stabilito dal Codice Privacy e che introducevano obblighi da questo non previsti. Avverso tale decisione del Tribunale, il Garante per la protezione dei dati personali ha presentato ricorso in Cassazione

2. *Le motivazioni della Corte di Cassazione*

La Corte di Cassazione ha ritenuto il ricorso fondato. Infatti, il Garante per la protezione dei dati personali ha evidenziato come le Linee guida citate non costituiscano un'integrazione dei precetti del Codice

¹ Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, "Linee guida in materia di attività promozionale e contrasto allo spam", 4 luglio 2013, paragrafo 2.6, disponibile all'indirizzo <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2542348>.

*Il consenso dell'Interessato come condizione per l'offerta di un servizio -
La sentenza della Corte di Cassazione 17278/2018*

La recente sentenza della Corte di Cassazione 17278/2018 pare porsi in contrasto con l'orientamento prevalente dei provvedimenti del Garante per la protezione dei dati personali in materia di libertà del consenso dell'interessato.

La questione affrontata nella sentenza in questione verteva sulla possibilità per il gestore di un sito Internet di condizionare la fruibilità dei servizi offerti al consenso dell'interessato per l'invio di comunicazioni commerciali. La Corte di Cassazione si è pronunciata in maniera favorevole, ritenendo che, in tali casi, il consenso non sia condizionato in quanto l'utente può liberamente ottenere il servizio in questione per altre vie.

Di diverso avviso è stato l'orientamento predominante del Garante per la protezione dei dati personali, il quale, nei provvedimenti precedenti, ha frequentemente sottolineato che il consenso che l'interessato 'deve' prestare quale condizione per conseguire la prestazione richiesta non può definirsi 'libero'. Tale posizione si riscontra analogamente anche nelle Linee Guida sul consenso ai sensi del Regolamento (UE) 2016/679 del Working Party, l'organo consultivo che riuniva i rappresentanti delle autorità di controllo in materia di protezione dei dati personali.

La posizione della nostra Corte Suprema può trovare la sua giustificazione nel tentativo di aprire all'attività di marketing diretto basata sull'interesse legittimo del Titolare del trattamento.

*Il consenso dell'Interessato come condizione per l'offerta di un servizio -
La sentenza della Corte di Cassazione 17278/2018*

The judgement of the Italian Supreme Court no. 17278/2018 seems to be in contrast with the prevailing orientation of the decisions of the Italian Data Protection Authority concerning the freedom of consent of Data Subjects.

The issue addressed in the judgement at stake concerned the possibility to subordinate the availability of the services offered through a website to the consent of the Data Subject to receive commercial communications. The Italian Supreme Court has ruled in favor, affirming that, in such cases, the consent is not conditioned. Accordingly, the user can freely obtain the same service by other means.

Different is the opinion of the Italian Data Protection Authority, which, in previous decisions, has frequently emphasized that the consent that a Data Subject must give as a condition to achieve the required service cannot be defined as "free". This position is also found in the Guidelines on consent of the Working Party, the advisory body that gathered the representatives of the supervisory authorities.

The position of the Italian Supreme Court may find its justification in the attempt to open to the direct marketing based on the legitimate interest of the Data Controller.

Il binomio digitale “*influencer-storytelling*”: la nuova pubblicità e la tutela dei consumatori

MARIATERESA FIOCCA*

«L'uomo è nato libero e ovunque si trova in catene.»¹

SOMMARIO: 1. Introduzione. – 2. L'*influencer* digitale e l'*influencer* marketing. – 2.1. Il baby *influencer*. – 2.2. L'*influencer* marketing. – 3. La *storytelling* digitale: la narrazione di consumo contemporaneo. – 4. I consumatori digitali: le nuove mosche in una bottiglia di vetro? Per una loro tutela. – 5. Conclusioni.

1. *Introduzione*

D'accordo, Rousseau faceva riferimento alla sfera politico-sociale nel passaggio appena citato, ma possiamo comunque avvalercene come metafora estremamente attuale nell'analisi che segue.

Obiettivo del presente contributo è l'esame del *digital social influencer* sulle scelte dei consumatori-*follower*.

Data la complessità del fenomeno, nel lavoro verrà utilizzato un approccio interdisciplinare che si estende all'economia, al diritto, alla psicologia, alle neuroscienze e alle tecniche di marketing (strategie di “brandizzazione”).

Uno dei primi capitoli di un manuale di microeconomia è tipicamente dedicato alla teoria delle scelte del consumatore. L'ipotesi di base è che ella/egli sia un agente economico razionale, vale a dire che massimizzi la propria utilità nell'acquisto di un paniere di beni di consumo, dati due vincoli: il proprio reddito e i prezzi di mercato dei beni stessi.

* Dirigente di ricerca (I livello), Istat. Componente del Comitato di Redazione della «Rivista di statistica ufficiale».

¹ Cfr. J.J. ROUSSEAU, *Il contratto sociale*, Libro I, cap. 1, 1762.

A scardinare le basi della teoria tradizionale un importante ruolo è stato assolto dalla neuroeconomia e, in questo specifico contesto, dal *neuromarketing*. Tramite gli esperimenti, vengono collegati economia, psicologia, neuroscienze e tecniche di marketing, in grado di individuare e monitorare cosa accade nel cervello del soggetto durante la sua esperienza di acquisto.

Uno degli importanti corollari è che, nel corso di una scelta di acquisto, i soggetti possono diventare in realtà del tutto irrazionali e trovarsi in balia di molteplici emozioni, evocazioni, ricordi, suggestioni, specifiche sensazioni. Cioè di *bias* che influenzano il loro processo decisionale. Essi assumono una “postura mentale” (per dirla *à la* Baricco²) che distorce il percorso del processo decisionale razionale – che probabilmente avevano già intrapreso³ – da cui essi si discostano al canto delle “sirene-*influenzer*”. È come se noi – continua Baricco⁴ – «avessimo iniziato a colonizzare zone di noi stessi che non avevamo mai esplorato e in parte neanche ancora generato».

Ne consegue l'importanza di contrastare – soprattutto sotto il profilo giuridico – tali pregiudizievoli distorsioni e interferenze e di creare una batteria di strumenti a tutela dei diritti e degli interessi effettivi dei consumatori digitali.

Dati il dilatarsi e il consolidarsi di tali strategie di marketing, che seguono velocemente l'evoluzione della tecnologia, il diritto deve cercare di stare al passo creando architetture di regolazione a tutela di questa specifica categoria di consumatori. Questione difficile e delicata perché la normazione di un fenomeno è spesso in affanno rispetto all'evoluzione del fenomeno stesso. E ciò è tanto più vero quando il fenomeno in questione ha forti componenti di tecnologia e di innovazione.

Ancor più arduo è un intervento *ex ante*, volto a prevenire fenomeni pregiudizievoli per i consumatori digitali, poiché in questo caso la legislazione deve anticipare i trend stessi (ad esempio, per il 2019 si prevede che i principali trend consistano nel consolidare i settori del *social listening*⁵,

² Cfr. A. BARICCO, *The Game*, Torino, Einaudi 2018, p. 14.

³ Ad esempio, ho bisogno del pane e quindi esco per andare al supermercato e, invece, torno a casa avendo acquistato un vestito anziché il pane.

⁴ *Ibidem*.

⁵ Monitoraggio delle conversazioni e dei commenti sui *social* su specifici argomenti, *brand*, frasi, parole chiave, ecc. per “auscultare” il proprio pubblico digitale e anti-

Il binomio digitale “influencer-storytelling”: la nuova pubblicità e la tutela dei consumatori

Il presente contributo ha l'obiettivo di esaminare i condizionamenti derivanti dalla diade “*digital social influencer-storytelling* digitale” sulle scelte dei consumatori-follower. *Influencer* (tra cui i *baby influencer*) e *storytelling* vengono in primo luogo analizzati separatamente e poi ricondotti in un unico alveo – data la loro stretta complementarità – per scandagliare le reciproche sinergie. Vista la poliedricità del fenomeno, il lavoro segue un approccio interdisciplinare esteso all'economia, alla psicologia, alle neuroscienze, alle tecniche di marketing, al diritto. Riguardo al diritto, le molteplici sfaccettature della brandizzazione tramite *digital social influencer* hanno aperto delicate questioni giuridiche riguardo alla tutela dei consumatori – ad ampio spettro, dall'inganno alla pubblicità negativa (che creano confusione nel consumatore e che si traducono in surrettizie pratiche di concorrenza sleale che inquinano il mercato), fino ai profili di *privacy*. Tuttavia – si sa – l'avanzamento della tecnologia è più veloce di quella della regolamentazione e tale *lag* temporale lascia nel frattempo il consumatore sprovvisto di adeguate difese.

La materia è ancora in divenire. Ciò per i tanti gangli della “*digitsfera*”, per l'innovatività degli strumenti *social* utilizzati e la velocità con cui questi vanno moltiplicandosi e diversificandosi, per gli elementi di oggettiva ambivalenza della materia stessa e della scivolosità del crinale in cui si muove.

Pivot nel settore della normativa della “brandizzazione” digitale a tutela della collettività sono stati gli USA. Ma anche in Italia, e più in generale nell'Unione Europea, la maggiore sensibilizzazione al fenomeno ha determinato progressi in tale direzione.

The digital “influencer-storytelling” duo: the new ways of advertising and consumer protection

The present paper aims at exploring the consumer-follower behavioural conditioning stemming from the digital “*influencer-storytelling*” duo. Influencers (including *baby influencers*) and *storytelling* are examined separately first and subsequently they are perceived as “complementary goods” achieving an overwhelming synergetic feedback. Given the complexity of such a digital phenomenon, the work implements a multidisciplinary approach: economics, psychology, neurosciences, marketing as well as law.

From the law viewpoint, because of the large number of aspects involved in brand strategies by means of digital social influencers, a wide range of issues aris-

es relating to consumer protection: from deception to negative advertising (confusing the consumer her/himself as well as recognised as a form of unfair competition) till very delicate aspects concerning consumer privacy. However – as it is well known – progress achieved in technology is faster than those ones achieved in regulation. Such a temporal lag leaves in the meantime the consumer devoid of any adequate defence.

The core of the matter is still in progress. This occurs because of the large number of knots relating the digital sphere, innovation in the social tools and speediness according to which they multiply and differ, the ambivalence of the field in itself and its slippery boundary. The pivotal experience in legislation on digital brand strategies is that one of United States. Yet, the moral suasion implemented by the regulator has achieved quite a few progress in the right direction also in Italy and, more in general, within the EU.

I dati personali in ambiente blockchain tra anonimato e pseudonimato

FRANCESCO RAMPONE*

SOMMARIO: 1. Introduzione. – 2. I dati in ambiente blockchain. – 3. La chiave pubblica. – 4. L'impronta hash. – 5. Coinbase e l'inserimento intenzionale di dati personali in blockchain. – 6. Titolari del trattamento in ambiente blockchain. – 7. Conclusioni.

1. *Introduzione*

Il Regolamento (UE) 2016/679 (GDPR), non diversamente dalla Direttiva 95/46/CE, ha un'impostazione prettamente centralistica, nel senso che esso contempla i trattamenti solo in una dimensione verticale, come operazioni che un soggetto (titolare) compie su dati personali altrui impiegando mezzi propri e scegliendo in autonomia lo scopo del trattamento e le misure di sicurezza adottate avvalendosi, all'occorrenza, di soggetti terzi fornitori di soluzioni informatiche o servizi di *data processing* (responsabili e sub-responsabili).

Al contrario, le soluzioni DLT – *Distributed Ledger Technology*, e in particolare la blockchain che di quelle è oggi la massima espressione, hanno uno sviluppo orizzontale, una natura sfuggente che non pare adattarsi alle disposizioni del Regolamento. Forse non tanto per un difetto di quest'ultimo, ma per un limite intrinseco alla architettura decentralizzata del fenomeno in esame, nel senso che una norma, quale essa sia, per sua struttura contempla sempre una condotta o una situazione di fatto o di diritto che permette l'individuazione di un soggetto a cui imputare la responsabilità. Una blockchain, invece, "agisce" per sintesi della volontà

* Dottoressa in Giurisprudenza presso l'Università degli Studi di Milano. Già laureata in Scienze politiche - Istituzioni e relazioni internazionali presso l'Università Cattolica di Milano.

di una moltitudine indeterminata di soggetti che interagiscono tra loro in modo anonimo e spesso anche inconsapevole del progetto globale a cui ubbidiscono, semplicemente eseguendo le linee di un codice *open source* che opera secondo un protocollo *peer-to-peer* dando origine a quello che qualcuno definisce un vero e proprio organismo¹.

Ebbene, se davvero la tecnologia blockchain è un nuovo Internet², se davvero dobbiamo credere che l'interazione decentralizzata tra utenti anonimi darà vita ad un sempre maggior numero di organizzazioni completamente autonome e separate rispetto alla volontà e alla responsabilità dalle persone fisiche che ne sono parte³, allora dobbiamo interrogarci sulla possibilità che la regolamentazione sulla protezione dei dati personali in ambiente blockchain giungerà presto al suo limite elastico oltre il quale saremo costretti a pensare a questa materia (ed evidentemente a molte altre) in termini completamente nuovi.

¹ Cfr. J. GARZIK, "Bitcoin, the organism", «TEDx Talk», Binghamton University, New York, 30 marzo 2014, definisce il bitcoin come un organismo e il suo lavoro di sviluppo come la ricerca di un biologo. Sulla stessa linea di pensiero si pone P. DE FILIPPI, "Blockchain Technology and the Future of Work", «Lift:Lab», Ginevra, 11 febbraio 2016, che paragona le DLT ai *plantoidi*, delle forme di protovita artificiale ideate e realizzate per la prima volta da un team di ricerca dell'IIT (Center for Micro-BioRobotics) di Pontedera. Più recentemente, M. FIELD, "The Blockchain Revolution: From Organisations to Organism", «TEDx Talk», Breda, 3 novembre 2016.

² Cfr. D.&A. TAPSCOTT, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World*, Portfolio/Penguin 2016, secondo i quali la blockchain rappresenta la seconda rivoluzione digitale dopo Internet: «*When decentralized blockchain protocols start displacing the centralized web services that dominate the current Internet, we'll start to see real internet-based sovereignty. The future Internet will be decentralized*» (seconda di copertina). Per altri, la blockchain si appresta a riconfigurare Internet in modo completamente nuovo: un Internet 3.0, dall'accesso a pagine statiche (1.0), ai contenuti *user generated* (2.0), alla costruzione di un network disintermediato (3.0). Per una rassegna di *blockchain evangelists*, Cfr. R. MARVIN, "Blockchain: The Invisible Technology That's Changing the World", PC Magazine 2017. Available at: <https://www.pcmag.com/article/351486/blockchain-the-invisible-technology-thats-changing-the-wor>.

³ Attraverso la blockchain si possono costituire delle organizzazioni decentralizzate (DAO – *Decentralized Autonomous Organization*) che hanno regole di governance e operano sul mercato attraverso l'esecuzione di linee di codice (*smart contract*). Essendo prive di organi di amministrazione e controllo e non ricadendo in alcun tipo legale (la natura di tali organizzazioni è molto dibattuta) in quanto sebbene le DAO non schermino dalla responsabilità diretta e illimitata dei loro partecipanti, questi, tuttavia, restano per lo più coperti dall'anonimato (lo stesso network di sviluppatori del protocollo bitcoin, il *BitcoinCore*, è una DAO). Per maggiori dettagli, Cfr. R.C. MERKLE, "DAOs, Democracy and Governance", *Cryonics Magazine*, July-August 2016, Vol. 37:4, pp. 28-40.

I dati personali in ambiente blockchain tra anonimato e pseudonimato

Le chiavi pubbliche e le impronte hash costituiscono le due soluzioni criptografiche fondamentali con cui costruire una blockchain. Esse sono considerate dati pseudonimi pressoché in modo unanime, ossia dati personali mascherati dietro un codice, ma che possono nondimeno essere attribuiti ad un individuo specifico con l'ausilio di informazioni aggiuntive. Se ciò fosse vero, lo sviluppo della tecnologia blockchain sarebbe minacciato dal rispetto delle disposizioni del Regolamento Europeo 2016/679 sulla protezione dei dati personali (GDPR). Con il presente lavoro, intendo invece dimostrare che alla luce della definizione di dato personale, anche in forma di dato pseudonimo, contenuta già nella Direttiva 95/46/CE e oggi nel GDPR, non è possibile qualificare come tale né la chiave pubblica né l'impronta hash per come sono effettivamente impiegate nel protocollo blockchain originale dei bitcoin (e quindi, in generale, in protocolli *permissionless* pubblici). Entrambe hanno infatti il solo scopo di risolvere un problema tecnico (il c.d. *double spending*), creando fiducia in un network con protocollo *peer-to-peer* e il loro eventuale utilizzo in sofisticate operazioni di *digital forensic* per rintracciare l'identità di titolari di indirizzi bitcoin, non le qualifica per ciò solo dati personali, né dati pseudonimi.

Personal data in blockchain environment between anonymity and pseudonymity

Public keys and hashes are the two fundamental cryptographic solutions commonly used to develop blockchain networks. They are considered almost unanimously pseudonymous data, that is personal data concealed behind an alphanumeric string that along with additional information can be nevertheless linked to a specific individual. If this were true, the development of blockchain technology would be hurdled by the necessity to comply with GDPR. In this paper, I held that the definition of personal data, even though in the form of pseudonymous data, set forth in Directive 95/46/EC and today in the GDPR (taking into account the CJEU interpretation and Article 29 Working Party opinion) does not apply neither to the public keys nor the hashes as they are used in a blockchain. They are not indeed used for concealing identities but to solve a technical problem (the so-called *double spending problem*) creating trust in a peer-to-peer network. Hence, although they could be (and sometimes they are) used to carry out advanced digital forensic searches to track down the identity of the private key holders, they are not actually designed to make or allow such searches and consequently they should be considered to be neither personal nor pseudonymous data.