Ciberspazio e diritto, vol. 20, n. 63 (3 - 2019), pp. 369-385

Le *fake news* e i danni da condivisione digitale in Italia*

Alba Calia**

Indice: 1. Le *fake news*. – 2. Le principali problematiche del sistema informativo digitale. – 3. La rilevanza nel quadro giuridico italiano della divulgazione online delle informazioni lesive dei beni giuridici. – 4. I danni da condivisione digitale. – 5. Conclusioni.

1. *Le* fake news

La divulgazione delle *fake news*, sebbene sia un fenomeno assai anteriore rispetto all'avvento del web e delle nuove tecnologie, ha recentemente assunto una più marcata rilevanza nel dibattito pubblico rappresentando una problematica dilagante soprattutto nel mondo dell'informazione digitale[1].

Il termine *fake news*, o nella corrispondente traduzione italiana *bufala*, è solitamente riferito a una notizia falsa o infondata, poiché riguardante un fatto mai accaduto, ovvero inesatta, quando invece viene deformato o travisato un fatto realmente avvenuto, che viene divulgata o perché ritenuta vera/esatta oppure con l'intenzione di trarre in inganno il lettore.

* Il presente scritto s'inquadra nel progetto di ricerca «Profili giuridici dell'automazione e delle nuove tecnologie – Teoria e pratica dei diritti soggettivi nei nuovi scenari tecnologici», finanziato dalla Fondazione di Sardegna.

** Avvocato, Cultrice di materia in Informatica giuridica e principi di filosofia del diritto presso l'Università degli Studi di Cagliari, Master di II livello in Diritto della Concorrenza e dell'Innovazione presso la LUISS School of Law.

[1] Il termine assume un'importante risonanza nel dibattito pubblico odierno a partire dal 2016 durante le elezioni presidenziali americane, quando la circolazione di notizie false in rete, secondo alcuni, avrebbero contribuito a decretare la vittoria di Donald Trump sulla sua avversaria Hillary Clinton.

Si precisa che il fenomeno non va esteso all'ambito del giornalismo professionale, che presuppone il rispetto di una serie di limiti al diritto di critica e di cronaca stabiliti dal relativo codice deontologico e oggetto di sistematizzazione grazie alla cosiddetta sentenza-decalogo del 1984 (Cass. Civ., sez. I, 18 ottobre 1984, n. 5259.)

La divulgazione di una *fake news* spesso avviene inconsapevolmente proprio perché si reputa, o si è indotti a credere[2], che il contenuto sia veritiero, anche sulla base del fatto che lo stesso viene condiviso da numerosi soggetti (i meccanismi che spiegano questa dinamica verranno descritti meglio nelle pagine a seguire). In altri casi si ha invece la consapevolezza e la volontà di diffondere un'informazione di cui si ha contezza della falsità o inesattezza[3]. Difatti, sono *fake news* anche quelle notizie create *ad hoc,* «intenzionalmente e verificabilmente false che potrebbero trarre in inganno i lettori»[4].

Ai fini della comprensione del fenomeno, è di ulteriore interesse lo studio degli eventuali scopi sottesi alla divulgazione di una *bufala* tra cui, ad esempio, la finalità di orientare le opinioni nel dibattito pubblico e politico; oppure ledere la reputazione e l'onore di un individuo o di un'azienda; la convalida di astruse ipotesi relative a fatti storici o a teorie complottiste; o, ancora, congetture o confutazioni scientifiche – o pseudo tali – con cui si indirizzano le convinzioni dei cittadini sull'affidabilità e sulla credibilità di una teoria in un determinato ambito della conoscenza, eventualmente in contrasto con le acquisizioni generalmente accolte dalla comunità scientifica[5].

In ragione delle finalità a cui è legata la diffusione, si distinguono due ipotesi di *fake news*: quelle non giuridicamente rilevanti, oppure quelle illecite, ossia lesive di un bene tutelato nell'ordinamento italiano. Più precisamente, l'illiceità di una *fake news* non deriva tanto dalla falsità in sé della notizia o dell'informazione divulgata, quanto dalla sua idonei-

[2] In tal caso, la distinzione consiste nel fatto che alcuni soggetti sin dal principio credono nella veridicità di una informazione (si pensi ai c.d. terrapiattisti o ai c.d. antivaccinisti), mentre altri, a seguito della diffusione di una bufala, vengono successivamente indotti a ritenere che un contenuto abbia una corrispondenza fattuale in quanto ne sono stati tratti in inganno.

[3] Cfr. M. Bassini, G.E. Vigevani, "Primi appunti su fake news e dintorni", «Rivista di diritto dei media» n. 1, settembre 2017, p. 16; Cfr. C. Melzi D'Eril, "Fake news e responsabilità: paradigmi classici e tendenze incriminatrici", «Rivista di diritto dei media», n. 1, settembre 2017, p. 63; Cfr. A. Mazziotti Di Celso, "Dal Primo Emendamento al bavaglio malese. Fake news, libertà di espressione e il rovesciamento delle categorie politiche tradizionali", «Rivista di diritto dei media», n. 3, ottobre 2018, pp. 98-99.

[4] Cfr. H. Allcott, M. Gentzkow, "Social Media and Fake News in the 2016 election", «Journal of Economic Perspectives», vol. 31, n. 2, 2017, p. 213.

[5] Cfr. F. Pizzetti, "Fake news e allarme sociale: responsabilità, non censura", «Rivista di diritto dei media», n. 1, settembre 2017, pp. 48 e ss.

Le fake news *e i danni da condivisione digitale in Italia*

Il saggio s'incentra sull'analisi del fenomeno delle *fake news* e sulle principali problematiche legate al panorama informativo digitale, quali la disintermediazione nella comunicazione, le *filter bubbles* e le *echo chambers*, nonché sul quadro normativo italiano in merito alla regolamentazione della diffusione di informazioni, false o vere ma non soggette a divulgazione, lesive di beni e interessi giuridici tutelati, come la reputazione individuale, la leale concorrenza o la salute pubblica. In tale contesto, si inserisce la nuova categoria concettuale di *danno da condivisione digitale* che denota i danni provocati dalla propalazione online, in particolar modo sui social network, di informazioni dannose, continuamente riproposte in maniera virale e persistente anche sfruttando le caratteristiche strutturali delle piattaforme digitali.

Fake news and harm from digital sharing in Italy

This paper is focused on the analysis of the fake news phenomenon and the main issues related to the digital information, such as disintermediation, filter bubbles and echo chambers. As well, this work analyses the Italian regulatory framework regarding the regulation of the concept of dissemination of informations, false or true but not subject to disclosure and detrimental of protected legal assets and interests (such as individual reputation, loyal competition or public health). In this context we want to include the new conceptual category of harm from digital sharing that denotes the damage caused by online propagation, especially on social networks, of harmful information, continuously reproduced in a viral way and taking advantage of the structural characteristics of digital platforms.

Ciberspazio e diritto, vol. 20, n. 63 (3 - 2019), pp. 389-413

Il consenso dei minori per i servizi della società dell'informazione sotto il profilo giuridico e informatico

Giacomo Bianchedi*

Indice: 1. Premessa. – 2. L'accesso dei minori ai servizi della società dell'informazione e il ruolo del consenso. – 2.1. La conclusione del contratto. – 2.2. Il trattamento dei dati personali. – 2.3. Gli obblighi imposti dal GDPR nella fornitura dei servizi della società dell'informazione ai minori. – 3. Le diverse soluzioni adottate e la compatibilità con il GDPR. – 3.1. L'età minima nei vari Stati membri. – 3.2. Le soluzioni adottate dai principali operatori del mercato. – 3.3. Riflessioni critiche sulle tecniche di verifica dell'età e/o dell'identità, anche alla luce delle esperienze maturate in altri settori. – 4. Conclusioni.

1. *Premessa*

Il presente lavoro mira ad approfondire il ruolo e i requisiti del consenso dei minori nell'accesso ai servizi della società dell'informazione, per poi operare una ricognizione circa l'adeguatezza delle principali soluzioni adottate rispetto alle prescrizioni del GDPR, per fornire infine spunti di riflessione e proposte operative.

La riflessione muove dalla constatazione che, a fronte della delicatezza del tema, l'accesso dei minori ai principali social network è tuttora scarsamente controllato, soprattutto con riferimento alla mancanza di verifiche circa la validità del consenso fornito dal minore, la veridicità dell'età indicata e l'effettiva legittimazione dei genitori a fornire il consenso nelle restanti ipotesi.

Oltre ai casi che hanno impegnato maggiormente l'opinione pubblica (si pensi ad es. a Cambridge Analytica), l'attenzione delle Authorities a livello mondiale si sta recentemente focalizzando anche sul tema

* Avvocato in Bologna. Ha frequentato con successo il Corso di Alta Formazione in Data Protection e Privacy Officer organizzato dall'Università di Bologna, a.a. 2018/2019, Direttore Prof. Avv. Fabio Bravo.

in esame, come ad esempio dimostra la sanzione da ultimo inflitta dalla US Federal Trade Commission (FTC) al servizio Musical.ly - Tik Tok (molto diffuso tra i ragazzi più giovani)[1], a cui è seguita l'apertura di una indagine da parte dell'Information Commissioner's Office (ICO) britannico[2].

Da quanto precede emerge pertanto la necessità di sensibilizzare maggiormente l'attenzione dell'opinione pubblica e degli esperti sul rispetto o meno dei diritti degli interessati da parte delle società i cui utenti sono in larga parte minori, come tali meritevoli di una tutela rafforzata della legittimità del trattamento dei propri dati.

Il presente lavoro si compone quindi di una prima parte prettamente giuridica in cui si analizza il ruolo del consenso nell'accesso ai servizi della società dell'informazione e si studiano i vari strumenti previsti dal GDPR a tutela dei diritti dei minori, a cui corrispondono specifici doveri in capo ai titolari del trattamento.

La seconda parte, invece, di natura più tecnica, si pone l'obiettivo di fornire un quadro delle principali soluzioni adottate dai maggiori operatori del mercato, analizzandone per ciascuna la compatibilità con le previsioni del GDPR e le eventuali criticità, per poi fornire delle proposte di sviluppo e una previsione circa la loro concreta realizzabilità.

2. *L'accesso dei minori ai servizi della società dell'informazione e il ruolo del consenso*

La versione definitiva del regolamento UE n. 2016/679 (GDPR), approvata all'esito del complesso *iter* legislativo[3], ha fortemente innova-

[1] Cfr. US Federal Trade Commission's press release of February 27, 2019, https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc, (16/09/2019).

[2] Cfr. Information Commissioner's Office, "The Information Commissioner's response to the Department for Digital, Culture, Media & Sport consultation on the Online Harms White Paper", 1 July 2019, https://ico.org.uk/about-the-ico/consultations/department-for-digital-culture-media-sport-consultation-online-harms-white-paper/, (16/09/2019).

[3] Cfr. M. Macenaite, E. Kosta, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?", *Information & Communications Technology Law*, vol. 26, n. 2, 2017, pp. 146-197; cfr. K. McCullagh, "The General Data

Il consenso dei minori per i servizi della società dell'informazione sotto il profilo giuridico e informatico

Il presente articolo esamina la compatibilità con il Regolamento UE 2016/679 (GDPR) delle principali soluzioni adottate per la verifica dell'età e della titolarità della responsabilità genitoriale rispetto a quelle disponibili sul mercato, al fine di fornire ai titolari del trattamento indicazioni utili nella scelta delle misure idonee per dimostrare di aver compiuto gli sforzi ragionevoli, anche alla luce della prassi della Federal Trade Commission statunitense nell'applicazione del Children's Online Privacy Protection Act (COPPA).

Child's consent in relation to information society services from legal and computer-science points of view

The paper examines the compliance with Regulation EU 2016/679 (GDPR) of the main solutions adopted to verify the age of the child or the identity of the holder of parental responsibility, compared to the available ones, in order to give useful indications to controllers when choosing the appropriate measures to demonstrate the reasonable efforts made, considering also the practice of the US Federal Trade Commission under the Children's Online Privacy Protection Act (COPPA).

Ciberspazio e diritto, vol. 20, n. 63 (3 - 2019), pp. 415-436

La responsabilità del provider al tempo dei *social network* (a un ventennio dalla Direttiva sul commercio elettronico)

Francesca Mollo*

Indice: 1. Il contesto di riferimento. – 2. La responsabilità del provider nel quadro precedente la Direttiva 2000/31/CE. – 3. La responsabilità del provider nell'impianto della Direttiva sul commercio elettronico 2000/31/CE. – 4. La responsabilità del provider nella modernità: il caso dei motori di ricerca. – 5. La responsabilità del provider nella post-modernità: il caso dei social network e delle piattaforme *TripAdvisor* e *Booking.com* – 6. Conclusioni.

1. *1. Il contesto di riferimento*

La figura del provider costringe l'interprete a fare i conti con illeciti calate in rete, spesso avvertita come uno spazio privo di padroni e regole[1], che annulla di fatto i confini geografici, e rende illimitate le potenzialità lesive della comunicazione così realizzata attraverso la propria perpetuità e immanenza[2].

Su Internet cambia non solo la quantità delle informazioni, ma la natura della loro comunicazione[3], dal momento che queste non sono solo varie, ma anche di facile reperibilità, spesso prive di contestualizzazione, ciò che le priva di un peso specifico ben definito, specialmente laddove la ricerca sia effettuata mediante motori di ricerca, che rappresentano, come si vedrà, un punto nodale oggi in tema di responsabilità del provider.

* Assegnista di Ricerca, Università degli Studi di Bologna.

[1] Cfr. S. Rodotà, "*Una costituzione per Internet?*"", in «Politica del diritto», n. 3, 2010, pp. 337-351.

[2] Interessanti sul punto le considerazioni in Trib. Trani, 24 novembre 2009, in «Dir. inf.», 2010, p. 261.

[3] V. Zeno Zencovich, "Comunicazione, reputazione, sanzione", in «Dir. informaz. e informatica», 2007, p. 266.

A partire dagli anni '90 si è assistito infatti ad un progresso vertiginoso, con la moltiplicazione dei *databases* e dei personal computer, la nascita di Internet, il moltiplicarsi di usi secondari dei dati personali, nel quadro di un vero e proprio *digital tsunami*[4] (e di conseguente "assalto alla privacy" a metà di quegli anni[5]).

D'altra parte, non è facile «giungere al cuore di Internet, coglierne la realtà vera, bisogna […] superare diffidenze, evitare trappole ideologiche, non restare abbagliato da quella che è stata chiamata la *Internet Trinity*».[6]

La questione della responsabilità del provider, d'altra parte, va letta alla luce di almeno tre fenomeni. In primo luogo, la globalizzazione[7], che

[4] S. Rodotà, "Controllo e privacy della vita quotidiana", in «Enc. giur. Treccani» .

[5] S. Rodotà, *Il mondo nella rete*, Bari, 2014, p. 7.

[6] S. Rodotá, *Libertà, opportunità, democrazie, informazione*, in *Internet e privacy: quali regole*, Atti del convegno, in Garante "cittadini e società dell'informazione" in supplemento I a Boll. n. 5, pubblicato da Presidenza del Consiglio dei Ministri - Dipartimento per l'informazione e l'editoria, p. 10.

[7] Cfr. F. Galgano., *La globalizzazione nello specchio del diritto*, Bologna, 2005; Id., "Diritto ed economia alle soglie del nuovo millennio", in «Contratto e Impresa», 2000, p. 189 ss; Id., *Lex mercatoria*, Bologna, 2001; Id., *Prefazione. Il volto giuridico della globalizzazione* e G. Alpa, *Postfazione*, entrambi in *Il contratto telematico*, a cura di V. Ricciuto e N. Zorzi, in *Tratt. dir. comm. e dir. pubbl. econ., diretto da Francesco Galgano*, Padova, 2002, vol. XXVII, rispettivamente alle pp. XIII ss. e pp. 345 ss.; P. Grossi, *Globalizzazione, diritto, scienza giuridica*, in P. Grossi, a cura di G. Alpa, Roma-Bari, 2011, p. 190 ss.; G. Alpa., "New economy e libere professioni: il diritto privato e l'attività forense nell'era della rivoluzione digitale", in «Contratto e Impresa», 2000, p. 1175 ss.; S. Rodotà, "Diritto, diritti, globalizzazione", in «Riv. Giur. Lav.», 2000; P. Barcellona, *Le passioni negate: globalismo e diritti umani*, 2001; N. Irti, "Le categorie giuridiche della globalizzazione", in «Rivista di diritto civile», 5, 2002, pp. 625 ss; N. Irti, *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari, 2001; ID., voce *Geo-diritto*, in *Enc. Treccani*, 2004; S. Rodotà, "Diritto, diritti, globalizzazione", in «Riv. giur. lav.»., 2000, n. 4; S. Cassese, *Il diritto globale. Giustizia e democrazia oltre lo Stato*, Torino, 2009; Id., voce *Globalizzazione del diritto*, in *Enc. Treccani*, 2009; M.R. Ferrarese, *Il diritto al presente. Globalizzazione e il tempo delle istituzioni*, Bologna, 2002; Id., *Le istituzioni della globalizzazione. Diritto e diritti nella società transnazionale*, Bologna, 2000; Id., *Prima lezione di diritto globale*, Roma-Bari, 2012. Sugli aspetti sociali ed economici della globalizzazione cfr. L. Gallino, *Globalizzazione e disuguaglianze*, Roma-Bari, 2003; Z. Bauman, *La solitudine del cittadino globale*, Milano, 2000; M.R. Ferrarese, *Le Istituzioni della globalizzazione. Diritto e diritti nella società transnazionale*, Bologna, 2000; W. Hutton, A. Giddens, *Global Capitalism*, The new press, New York 2000; A. Giddens, *Il mondo che cambia: come la globalizzazione ridisegna la nostra vita*, Bologna, 2000; G. Teubner (a cura di), *Global Law without a State*, Dartmouth, Adelrshot-Brookfield USA-Singapore-Sidney, 1997; J. Ziegler, *La privatizzazione del mondo*, Milano 2003; J. Osterhammen

La responsabilità del provider al tempo dei social network *(a un ventennio dalla Direttiva sul commercio elettronico)*

Il contributo intende delineare i confini della responsabilità del provider, a partire dal riferimento normativo costituito dalla Direttiva 2000/31/CE, ormai risalente a inizio millennio, per verificarne, anche alla luce dell'evoluzione precedente e successiva, la perdurante attualità.
In quest'ottica si colloca anche l'analisi degli orientamenti della giurisprudenza, in particolare della Corte di Giustizia, in tema di motori di ricerca e hosting provider attivo e passivo.
Da ultimo, si affronta il caso dei social network e delle piattaforme *user generated content*, in particolare *TripAdvisor* e *Booking.com* sotto il profilo della responsabilità del provider.

Internet provider's responsibility in the age of social networks (twenty years after the e-commerce directive)

The contribution intends to delineate the boundaries of the provider's responsibility, starting from the normative reference established by Directive 2000/31/EC, dating back to the beginning of the millennium, to verify, also in the light of the previous and subsequent evolution, the ongoing relevance. In this perspective, the analysis of the guidelines of the jurisprudence, in particular of the Court of Justice, is placed in terms of search engines and active and passive hosting providers. Finally, the case of social networks and user generated content platforms is addressed, in particular TripAdvisor and Booking.com in terms of provider responsibility.

Ciberspazio e diritto, vol. 20, n. 63 (3 - 2019), pp. 437-461

"Internet never forgets"(?). Diritto all'oblio e diritto alla cancellazione, quali gli usi e quali i limiti*

Giuseppe Lavacca, Carlo Maria Artini, Michelangelo Pellegrino

Indice: 1. Breve introduzione del concetto di diritto all'oblio. – 2. Il caso Węgrzynowski e Smolczewski vs. Polonia: bilanciamento fra l'art. 8 e l'art. 10 CEDU. – 3. La sentenza della Corte di Giustizia U.E. (causa C-131/12): il c.d. caso Google Spain e le sue implicazioni. – 4. Il caso Fuchsmann vs. Germania: breve raffronto del diritto all'oblio con l'art. 8 CEDU. – 5. La posizione della Corte di Cassazione in merito al bilanciamento fra il diritto all'oblio ed il diritto alla cronaca: dalle sentenze del 1984 ad oggi. – 6. Analisi e considerazioni circa l'art. 17 GDPR. – 7. Conclusioni.

1. *Breve introduzione del concetto di diritto all'oblio*

Right to be forgotten ovvero il diritto all'oblio, il diritto di non sapere o, in una accezione moderna "il diritto a non essere tracciato"[1], è un'espressione conosciuta e diffusa in tutti gli ambienti, giuridici e non. L'e-

* Il presente lavoro è da considerarsi un'opera corale di tutti e tre gli autori, tuttavia sono da attribuirsi a ciascuno degli stessi i seguenti paragrafi. G. Lavacca: parr. 1; 6; 7. C.M. Artini: parr. 3; 4; 7. M. Pellegrino: parr. 2; 5; 7.

Giuseppe Lavacca si è laureato in giurisprudenza nel 2017 presso l'Università di Pisa, ha conseguito il Master di I° livello in Giurista dell'economia e manager pubblico presso l'Università di Pisa nel 2018, ha frequentato il corso "Data Protection e Privacy Officer" presso l'Università di Bologna nel 2019. Lavora come Assistant Account presso primaria società a livello mondiale nella consulenza dei rischi e delle risorse umane.

Carlo Maria Artini si è laureato in giurisprudenza nel 2015 presso l'Università di Pisa. Ha conseguito nel 2018 l'abilitazione alla professione forense. Attualmente, è il legale interno di una primaria società informatica italiana.

Michelangelo Pellegrino si è laureato in giurisprudenza presso l'Università di Bologna nel 2018, ha frequentato il corso "Data Protection e Privacy Officer" e, attualmente, si occupa di contenzioso civile, privacy e finanza agevolata presso uno studio legale di Rimini. È madrelingua italiano e polacco.

[1] Cfr. S. Rodotà, *Il mondo nella rete, Quali diritti, quali vincoli*, Roma-Bari, Laterza, 2014, p. 41.

"Internet never forgets"(?). Diritto all'oblio e diritto alla cancellazione, quali gli usi e quali i limiti

"Internet never forgets": questo è il punto di partenza per un'analisi sul diritto alla cancellazione dei dati (il c.d. diritto all'oblio) presente nel Regolamento 679/2016, meglio noto come GDPR.
Negli ultimi anni, la rete ha assunto le caratteristiche di un sistema di memorizzazione implementabile e, allo stesso tempo, consultabile da tutti come una memoria condivisa nella quale immettere i propri ricordi. Ricordi che, una volta inseriti, iniziano a viaggiare sulla rete tramite continue condivisioni.
Nel contesto di un Internet nel quale il passato è sempre presente, nasce l'esigenza di un diritto capace di permettere la ri-appropriazione delle proprie informazioni o, quanto meno, di un loro controllo. Il diritto all'oblio nasce come la lecita esigenza di risultare invisibile in rete o, meglio, di non essere ricordato.
Alla luce di queste considerazioni, il presente lavoro si pone l'obiettivo di investigare sulle origini del diritto all'oblio, compiendo una ricerca dottrinale e giurisprudenziale in merito alla sua affermazione come diritto prima e dopo della diffusione di Internet, fino a giungere alla definizione che ne dà il nuovo Regolamento Europeo sulla protezione dei dati personali.

"Internet never forgets"(?). Right to be forgotten and right to erasure, its purposes and limits

"Internet never forgets": that is our starting point in order to analyse the right to be forgotten pursuant to the EU Regulation n. 679/2016, best known as GDPR.
Nowadays the web has become an implementable storage system, which everyone can consult as if it were a shared memory in which you can enter your memories.
Memories that, once inserted, begin to travel on the net through continuous sharing.
In a place like the Internet where the past is always present, we need a right capable of regaining our data or, at least, of controlling it. For these reasons the right to be forgotten arises as the legitimate demand to be invisible in the net or, better, not to be remembered.
In light of the above, this paper will analyse the history and the law cases concerning the right of erasure before and after the Internet spreading. It will also be considered the definitions provided by GDPR and the consequences of these changes in legislation.

spressione è connessa all'immagine della cancellazione, del rendere invisibile qualcosa che naviga nella rete di Internet, ma non è così. O meglio, il diritto all'oblio nasce e si sviluppa prima della rete, e vede scontrarsi fin dagli albori della sua definizione con il diritto di cronaca, baluardo delle odierne democrazie.

Dalla *damnatio memoriae*, antica tecnica sociale di condanna delle azioni nefaste che tanto hanno macchiato il tessuto sociale di appartenenza, si è passati ad una *damnatio* rappresentata dalla conservazione eterna delle informazioni[2].

Nato, prima dell'avvento di Internet, in Francia come "*droit à l'oubli*"[3], si colloca nell'ambito dei diritti della personalità[4], assediato fin da subito dal quesito che ne fa da antifona: quando, le vicende passate rese pubbliche in maniera del tutto lecita, possono essere nuovamente divulgate a fini di cronaca e quando, invece, la nuova divulgazione con il trascorrere del tempo diviene illecita.

In Italia, invece, la prima apparizione in dottrina del "diritto all'oblio" risale al 1983 in un saggio di Auletta[5] in cui si sostiene che «si tenta di conferire rilievo, e dunque tutela giuridica, all'interesse di un soggetto (le cui vicende furono un tempo note, perché ampiamente diffuse e pubblicizzate) a rientrare nell'anonimato».

La sua consacrazione formale in giurisprudenza avviene però nel 1996 presso il tribunale di Roma[6], e successivamente nel 1998 presso la Suprema Corte di Cassazione[7].

[2] *Ibidem*, p. 42.

[3] Cfr. G. Lyon-Caen, «La Seimane Juridic», 1966 n. 14482. Si tratta di un episodio di cronaca nera riguardante il "serial killer" francese H. Landru, reo di aver brutalmente assassinato le proprie amanti.

[4] Cfr. Dichiarazione Universale dei Diritti dell'Uomo, 10 dicembre 1948, art. 12; Convenzione Europea dei Diritti dell'Uomo, 4 novembre 1950, art. 8, comma 1.

[5] Cfr. T.A. Auletta, *Diritto alla riservatezza e "droit a l'oubli*, in *L'informazione e i diritti della persona,* G. Alpa, M. Bessone, L. Boneschi, G. Caiazza (a cura di), Napoli, Jovene Editore 1983.

[6] Cfr. A. Savini, "Diritto all'oblio e diritto alla storia*"* (nota a ord. Trib. Roma, 20 novembre 1996), «Il Diritto di Autore», n. 3, 1997, pp. 372 ss. Secondo l'interpretazione del tribunale, il diritto all'oblio pur rientrando nell'ambito della tutela della vita privata, è volto «*ad impedire che fatti già resi di pubblico dominio (e quindi sottratti al riserbo) possano essere rievocati – nonostante il tempo trascorso e il venir meno del requisito dell'attualità* […]».

[7] Cfr. P. Laghezza, "Il diritto all'oblio c'è (e si vede)" (nota a Corte di Cassazione n. 3679/1998), «Foro Italiano», fasc. I, 1998, p. 1834.

Ciberspazio e diritto, vol. 20, n. 63 (3 - 2019), pp. 463-472

Il *machine learning* per la sicurezza delle informazioni: un approccio *metodico-procedurale* per l'analisi delle verifiche delle misure tecnico-organizzative per la protezione dei dati

Onofrio Signorile*

Indice: 1. Introduzione. – 2. Definizione della metodica. – 3. Definizione e raccolta dei dati. – 4. Apprendimento della struttura e processo di inferenza. – 5. Conclusioni.

1. *Introduzione*

Esiste una lunga serie di statistiche relative ad accessi abusivi a sistemi informatici finalizzati a trafugare indebitamente i dati ed una lunga serie di motivi che possono spingere un dipendente o un *insider* a trafugare i dati. Ciò in organizzazioni medio-grandi è un fenomeno difficile da controllare se non ad incidente avvenuto. Spesso la difficoltà è insita nel fatto che il potenziale intruder dispone "lecitamente" delle autorizzazioni necessarie per accedere ai dati. Pertanto, ci si ritrova a dover implementare politiche di sicurezza che vedono contrapposte esigenze di accesso ai dati per necessità lavorative e livelli di sicurezza sempre più stringenti che tendono a limitare l'utente negli accessi: Principio del minimo privilegio.

In tale ambito, negli ultimi anni è emersa un'esigenza sempre più forte di costruzione di adeguati sistemi di controlli interni per ottimizzare la gestione dei rischi e adeguarsi alle normative che responsabilizzano i vari attori coinvolti. La materia è ampiamente argomentata da una serie di norme, alcune delle quali vincolanti altre volontarie.

In questo lavoro si cercherà di delineare un modello procedurale-generale per il presidio del rischio utilizzando, nello specifico, l'analisi dei dati di *audit* riferibili a fenomeni che possano determinare responsabilità

* Ingegnere dell'Informazione, perfezionato in Digital Forensics presso l'Università degli Studi di Milano. Si occupa prevalentemente di sicurezza delle informazioni e delle reti nonché di applicazioni di Intelligenza artificiale per l'analisi del rischio.

dall'uso illegittimo dei dati. A titolo di esempio sarà analizzato il processo di *audit* relativo alla verifica delle politiche di attribuzione delle abilitazioni per l'accesso ai Sistemi Informatici aziendali; rischio di *data leak* da parte di utenti *Opportunistic Insider*[1].

Sotto opportune ipotesi il modello può essere generalizzato all'intero processo di *audit* di verifica dell'attuazione delle misure tecnico-organizzative, laddove il fattore umano risulta essere rilevante nell'intero processo.

Sarà mostrata l'analisi dei dati di *audit* mediante l'utilizzo delle tecniche di *machine learning* e modelli analitici. L'idea di base è fornire un modello di apprendimento automatico in grado di produrre risultati affidabili e replicabili.

2. *Definizione della Metodica*

Esistono diverse linee guida per le attività *audit* per ottenere evidenze e valutare con obiettività il rispetto dei criteri di *compliance* implementati. A ciò va aggiunto, inoltre, la capacità degli auditor di individuare ulteriori indizi dai colloqui informali, che saranno poi utilizzati per indirizzare l'attività d'indagine nella corretta direzione. Il contributo maggiore è offerto dall'esperienza, dalla multidisciplinarietà e dalla pro-attività dei soggetti agenti. Ciò deriva anche, dall'esistenza di un numero imprecisato di *variabili* che influiscono sulla capacità di correlazione e analisi delle informazioni acquisite. È possibile individuare due importanti variabili che ne influenzano i risultati: la variabile *procedurale* e la variabile *soggettiva.*

La prima, *procedurale*, è legata sia alle caratteristiche della metodica utilizzata sia "*all'ambiente*" nel quale l'attività viene svolta. Si pensi ad esempio, all'attività di *audit* di conformità ai requisiti tecnici e di sicurezza degli apparati IT.

La seconda variabile, *soggettiva,* è correlata con i rischi da presidiare e quindi con gli obiettivi di ciascun *soggetto/attore di riferimento coinvolto* in relazione ai requisiti del Sistema di gestione implementato (rischi di business, rischi informativi, rischi di processo, ecc.).

[1] Utenti che non commettono azioni fraudolente per ottenere i privilegi di accesso, ma dispongono già di privilegi superiori a quelli necessari.

Il machine learning *per la sicurezza delle informazioni: un approccio metodico-procedurale per l'analisi delle verifiche delle misure tecnico-organizzative per la protezione dei dati*

In questo articolo si propone una metodica generale-procedurale, al fine di definire una possibile applicazione interdisciplinare tra modello di audit e *machine learning*.

Machine learning *for information security: a methodical-procedural approach to the analysis of the verification technical and organisational measures for data protection*

In this article a general-procedural method is proposed, in order to define a possible interdisciplinary application between the audit model and *machine learning*.

Ciberspazio e diritto, vol. 20, n. 63 (3 - 2019), pp. 475-494

Il *darkside* del cosmo digitale: "bersaglio-giovani". Le tutele

Mariateresa Fiocca*

Indice: 1. Introduzione. – 2. Burattini & burattinai digitali: giovani a rischio-cyber malato. – 3. La manipolazione attraverso il *framing effect* e altri *bias* cognitivi nel cyber. – 4. Le buone pratiche social. – 5. Conclusioni.

1. *Introduzione*

Il contributo analizza la manipolazione via cyber a danno dei giovani attraverso il *framing effect* e altri *bias* cognitivi che mutano la struttura soggettiva delle preferenze e degli incentivi. Per sua natura, l'uomo convive con i *bias*. La convivenza è ancor più stretta se alla creazione delle anomalie cognitive concorre la manipolazione. Convivenza e connivenza. Di seguito si ipotizza che vittime dei *bias* siano prevalentemente i giovani per via del funzionamento della mente, qui colto dalla metafora di Kahneman[1] nell'interazione fra due sfere cognitive – "Sistema 1" e "Sistema 2" –, e nel prevalere dell'una sull'altra (par. 3). Naturalmente, paradossi della *social network society* (par. 2) con protagonisti i giovani non sono attribuibili solo a *bias*. Spesso i disagi sono profondi e complessi. Una corrente psicoanalitica sostiene che l'abuso di nuove tecnologie fra giovani si presta all'evitamento del dolore mentale – dato dalla complessità del rapporto con la propria sfera interiore e con il prossimo –, induce al soddisfacimento del bisogno costante di disponibilità e di gratificazione, favorisce lo sviluppo di un sé grandioso, è un "rifugio" della mente favorevole al manifestarsi di aspetti di sé (anche sofferenti). Quando i *bias* si intrecciano al malessere giovanile, verosimilmente si alimentano reciproche sinergie perverse.

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

[1] Cfr. D. Kahneman, *Pensieri lenti e veloci*, Milano, Mondadori, 2012.

Nel lavoro è adottata la geometria: "cyber – giovani – manipolazione – *bias* cognitivi – *framing effect*". Pur usando un approccio interdisciplinare, ci si avvale soprattutto dell'economia cognitiva. Le violazioni al paradigma neoclassico della razionalità economica – ottimizzante e onnisciente – sono sistematiche. Il *modus operandi* dei soggetti non procede secondo la lineare razionalità neoclassica, ma devia per scorciatoie e rappresentazioni "abbreviate" della realtà. Tale riconoscimento porta alla centralità degli aspetti cognitivi ed emotivi dei processi decisionali, collegando psicologia ed economia. L'economia cognitiva riformula la teoria innestando nel suo alveo robusti principi (identificati e verificati via lab) che rappresentano fatti stilizzati nel comportamento dei soggetti. Economia cognitiva, economia sperimentale (basata su esperimenti controllati in lab), neuroeconomia[2] ed economia comportamentale sono dunque contigue, avvalendosi di *cross-fertilisation.* Un importante ruolo qui assume pure l'economia dell'informazione. Possono ricondursi al suo *mainstream* la disinformazione online – fake news immesse e rilanciate nelle piattaforme artatamente a fini manipolatori o inconsapevolmente dagli utenti[3] – e la privacy – tutela di informazioni personali, valore e costo della tutela. La privacy ha quindi valenza giuridico-legale[4] ed economica. Nel 2010 Zuckerberg tentò di ridurne il valore: «Ormai gli utenti condividono senza problemi le informazioni personali online. Le norme sociali cambiano nel tempo. E così è anche per la privacy». Per il tecno-capitalista massimizzare i profitti significa sfruttare l'innata socialità dell'uomo e l'esposizione di sé; i dati personali (cioè la vita dei giovani utenti) sono input acquisiti con la surrettizia offerta di una vita *user-fliendly*, la retorica della condivisione e la componente ludica. Errore! Nel 2019 a San Jose

[2] Usa le tecniche di *neural imaging* per evidenziare le aree del cervello stimolate nella risposta a specifici compiti di scelta. Tali procedure individuano empiricamente i modelli neurocognitivi del ragionamento e del processo decisionale.

[3] Alcuni ricercatori del MIT in uno studio – considerato il più grande e sistematico sulle fake news – hanno scoperto che una fake su Twitter ha il 70% di probabilità in più di essere retweettata di una "*true*". Inoltre, quando si considerano le c.d. "cascate" di Twitter, cioè le catene di condivisione, le falsità sono da 10 a 20 volte più veloci della verità. Questo vale pure quando a retweettare non sono bot, ma persone. Cfr. S. Vosoughi, D. Roy, S. Aral, "The Spread of True and False News Online", «Science», vol. 3599, issue 6380, March 2018, pp. 1146-1151.

[4] Cfr. il Regolamento (UE) n. 2016/679 (GDPR - *General Data Protection Regulation*), in tema di trattamento dei dati personali e di privacy, adottato il 27 aprile 2016 e operativo dal 25 maggio 2018.

Il darkside del cosmo digitale: "bersaglio-giovani". Tutele

Il contributo esamina come la manipolazione via cyber agisca a danno dei giovani mediante il *framing effect* e altri *bias* cognitivi. Pur usando un approccio interdisciplinare, l'analisi si avvale soprattutto dell'economia cognitiva. Un importante ruolo assume pure l'economia dell'informazione: può ricondursi al suo *mainstream* la disinformazione online e la tutela della privacy. Nel lavoro si ipotizza che vittime dei *bias* siano prevalentemente i giovani per via del funzionamento della mente, colto dalla metafora di Kahneman, nell'interazione fra le due sfere cognitive: "Sistema 1" e "Sistema 2".
Tra i numerosi *bias* analizzati, assume ruolo centrale nel lavoro il *framing effect*, di cui i giovani possono cadere facili prede attraverso un'artata architettura manipolatoria nella presentazione del set di scelte loro disponibili.
La tutela richiede numerosi strumenti – come le *policy* fondate sulla "spinta gentile" – e molti attori: dai player della galassia social, al legislatore internazionale e interno, alla società civile, alla sanità, a scuola e famiglia.

The darkside of the digital cosmos: "targeting young people". Safeguards

The present paper aims at exploring how manipulation via cyber damages young people through the framing effect and other cognitive biases. An interdisciplinary approach is here adopted, mainly by using the cognitive economic theory. A relevant role is also played by the information economics (fake news and privacy). The Kahneman's idea – the two mental spheres: "System 1" and "System 2" – is followed to explain why young people are major victims of biases and framing effect via cyber. Their effective safeguard requires a number of policy measures (e.g. *nudging*) to be implemented and many actors to be involved.

Ciberspazio e diritto, vol. 20, n. 63 (3 - 2019), pp. 495-516

Il nuovo spazio tra dimensione analogica e digitale. Riflessioni su sicurezza, libertà e un caso pratico: l'*online advertising* e *Myntelligence*

Dario Antares Fumagalli[*]

Indice: 1. Il Big Bang tecnologico e la nascita di un nuovo spazio. – 2. Nuovi orizzonti per la sicurezza collettiva e individuale. – 3. La bilancia e la spada. – 4. Un caso di studio: la pubblicità online e *Myntelligence.* – 5. Conclusioni.

1. *Il Big Bang tecnologico e la nascita di un nuovo spazio*

Come spesso accade, i grandi passaggi storici, gravidi di conseguenze dirompenti sul piano scientifico, culturale, sociale ed economico hanno una radice geografica[1]. Le rivoluzioni spaziali, infatti, frantumando gli schemi gnoseologici e i modelli sociali preesistenti, sono sempre state foriere di sfide la cui soluzione ha comportato enormi opportunità di evoluzione per le comunità coinvolte[2]. Anche la fase storica attualmente in corso, che noi stessi percepiamo come profondamente rivoluzionaria, è caratterizzata – a ben vedere – da una genesi di natura geografica[3].

[*] Laureato in Giurisprudenza all'Università Statale di Milano – Bicocca e ha conseguito il Master in Geopolitica e sicurezza globale presso l'Università Sapienza di Roma, da circa due anni è attivo nel settore della data protection come autore di articoli e operatore specializzato. Consulente presso il Consiglio d'Europa per il redigendo Rapporto "Need for democratic governance of artificial intelligence".

[1] «Nella storia delle relazioni internazionali, […] i grandi mutamenti hanno coinciso quasi sempre con rivoluzioni spaziali», cfr. A. Colombo, *La disunità del mondo. Dopo il secolo globale*, Milano, Feltrinelli, 2010, p. 62.

[2] Cfr. F. Farinelli, *Geografia. Un'introduzione ai modelli del mondo*, Einaudi, Torino, 2003, p. 8, p. 121 e p. 158.

[3] Occorre soffermarsi brevemente sul significato che, in questa sede, si vuol ricondurre all'aggettivo "geografica". Carlo Jean definisce la geografia come "descrizione di un dato momento storico" Cfr. C. Jean, *Geopolitica del mondo contemporaneo*, Roma, Laterza, 2012, p. 3, riassumendo così tutti gli aspetti che l'analisi geografica prende in considerazione, ovvero, come espresso da Farinelli, «il complesso delle relazioni (sociali, econo-

Sarebbe infatti superficiale far coincidere l'originalità del passaggio storico contemporaneo con il solo sviluppo dell'informatica. Ciò che, piuttosto, ha segnato l'alba di una nuova era tecnologica è stata la creazione di un nuovo ambiente delle attività e relazioni umane, in altri termini di un nuovo spazio. Occorre fin da subito chiarire, però, che questo nuovo spazio non è quello che, comunemente, definiamo *cyberspace*[4] Quest'ultimo, infatti, ne è elemento costitutivo, ma non ne riassume l'essenza. Il nuovo spazio è quello generatosi dallo sviluppo di fenomeni tipici della fusione, ormai quasi completa, tra spazio digitale e spazio analogico. Ne percepiamo l'esistenza tutti i giorni attraverso la nostra esperienza, laddove proiettiamo la nostra vita, senza soluzione d continuità, tra strada e social network. Tuttavia, così come non potremmo descrivere una regione geopolitica come la mera somma delle terre e dei mari ricompresi entro il suo perimetro e dei fenomeni socioeconomici in essa radicati, non possiamo descrivere lo spazio entro il quale oggi si sviluppano le nostre attività e relazioni come la mera somma di ciò che è relativo allo spazio analogico e ciò che è relativo al *cyberspace*. Più opportuno sarebbe concepirne uno nuovo, nel quale collocare fenomeni, problemi e relazioni tipiche che si sviluppano secondo regole e coordinate del tutto diverse rispetto al passato. Parliamo, dunque, di un nuovo spazio, nel caso di specie politico[5]. L'aggettivo "politico" riferito allo spazio è ispirato, in questa sede, alle riflessioni in materia proposte, ormai quasi dieci anni fa, da Alessandro Colombo[6]. Se, tuttavia, l'idea espressa dall'au-

miche, politiche, culturali) al cui interno si svolge la vita umana». Cfr. F. Farinelli, ivi, p. 6. In sintesi, la nozione è quella tramandata da Carl Ritter, per mezzo del termine tedesco *Erdkunde,* traducibile come «conoscenza storico-critica della Terra».

[4] Per una riflessione in merito alla natura del *cyberspace* sotto il profilo politico particolarmente approfondita si veda G. Suffia, *Geografia delle cyberwars. Uomini e Stati alla prova dello spazio digitale,* Milano, Giuffré, 2018, alle pp. 1-21.

[5] Dove per politico si intende relativo allo sviluppo dei fenomeni relazionali umani e in particolare nel quale possano evolvere le dinamiche connesse alla conquista, alla conservazione e alla distribuzione del potere, richiamando la definizione che dell'aggettivo politico ha dato Max Weber in "Wissenschaft als Beruf. Politik als Beruf", cfr. M. Weber, *La scienza come professione. La politica come professione*, Torino, Einaudi, 2004, p. 49.

[6] Il quale attribuisce alla locuzione tre possibili significati. In un primo significato, due attori appartengano a uno stesso spazio quando l'uno non può prescindere dalle azioni dell'altro nelle proprie decisioni. In un secondo caso, l'Autore considera che due attori appartengano a uno stesso spazio politico laddove, «consapevoli di interessi e valori comuni, si preoccupino di soddisfare almeno gli obiettivi elementari di qualunque convivenza sociale: il mantenimento delle promesse, la stabilizzazione del possesso e la limi-

*Il nuovo spazio tra dimensione analogica e digitale. Riflessioni su sicurezza, libertà e un caso pratico: l'*online advertising *e* Myntelligence

L'articolo prende le mosse dalla riflessione secondo cui la rivoluzione digitale avrebbe condotto alla nascita di un nuovo spazio dell'umano agire, foriero di opportunità e rischi tipici, inferendo quindi la necessità di mitigare questi ultimi mediante la giustapposizione agli interventi di natura giuridica di una strategia di intervento che passi per soluzioni pratiche, vantaggiose e sicure. L'analisi prosegue focalizzandosi, in ottica sperimentale, sul settore del *programmatic advertising* online, individuandone i profili d'interesse e di problematicità, concludendo con il vaglio di una specifica soluzione di *advertising* oggi adottata da numerose organizzazioni anche rilevanti per il network nazionale, la piattaforma *Myntelligence*.

The new space between analogic and digital dimension. Considerations on security, freedom and a case study: online advertising and Myntelligence

The article opens with a reflection about how the digital revolution has given birth to a new space for the human activity that is harbinger of opportunities and typical risks. Then, the author argues that, in order to mitigate the above-mentioned risks, it is necessary to juxtapose laws with a strategy made of advantageous practical solutions. The article goes on focusing, in an experimental way, on the online programmatic advertising, identifying the relevant profiles of concern and troubles. The article concludes with the analysis of a specific solution adopted today by a lot of big Italian companies: *Myntelligence* platform.