GIURISPRUDENZA E DIRITTO

a cura della Fondazione Aiga Tommaso Bucciarelli

F. Colapaoli, A. Coppola, F.R. Graziani
M. Mirone, M. Zonaro

SOCIAL NETWORK E DIRITTO

G. Giappichelli Editore

Prefazione
Cambio di paradigma

Francesco Giorgino *

Sono due le ragioni per le quali è importante che venga pubblicato un libro sul rapporto tra i social network e il diritto. La prima è relativa all'esigenza di strutturare questa dinamica relazionale considerando sia il piano fenomenologico, sia quello ontologico. La seconda è dovuta al fatto che anche questa occasione è utile per ribadire il valore di un approccio analitico non solo di tipo multidisciplinare, ma anche transdisciplinare. E ciò, attingendo sia alle scienze giuridiche (com'è nelle competenze specifiche degli autori del volume che il lettore ha tra le mani) sia alle scienze sociali (com'è invece nella sensibilità di chi firma la prefazione).

Tra le scienze sociali un ruolo di primo piano lo svolge la sociologia, che per statuto epistemologico ha il compito di studiare l'interazione nella società, a livello macro e micro. Si può seguire sia la traiettoria concettuale della sociologia della comunicazione, sia quella della sociologia del diritto. Si tratta di un modo utile a individuare i *touch point* esistenti tra i due ambiti teorico-empirici nei quali si articola il percorso concettuale di questo lavoro.

La sociologia della comunicazione ha gli strumenti utili per indagare il fenomeno dei social network in base a tre variabili: l'influenza della società sui media; le tecniche e le modalità di produzione e ricezione dei contenuti ad opera di questi strumenti di comunicazione dell'era del digitale; l'influenza dei media (vecchi e nuovi) sulla società e, quindi, sugli individui e sulla collettività, considerando gli effetti cognitivi, emozionali e conativi che si generano e si rigenerano come conseguenza della ricerca spasmodica della simmetricità.

In ordine alla prima variabile è opportuno riferirsi alla *platform society* (Van Dijk, 1999), categoria in base alla quale è possibile evidenziare la capacità delle piattaforme di plasmare le società occidentali tardo-moderne, coltivando valori riconducibili a fattori esogeni (la *digital transformation*) ed endogeni di matrice so-

---

* Francesco Giorgino, giornalista e professore Luiss dove insegna Content Marketing & Brand Storytelling e Newsmaking. Dirige presso la Luiss School of Government il Master di secondo livello in Comunicazione e Marketing politico ed istituzionale. È autore di decine di saggi e paper scientifici sui temi della comunicazione, dell'informazione e del marketing.

cio-culturale come, per esempio, l'individualismo libertario, la desocializzazione, la fruizione de-sincronizzata dei contenuti (Beck, 2000). In ordine alla seconda variabile il riferimento è ai temi della *privacy*, della sicurezza e protezione dei dati, ma anche a quelli dell'equità, dell'accessibilità e del controllo democratico. Sono elementi che documentano quanto sia alta la posta in palio. Sono questioni che evocano una riflessione (come del resto si fa in modo articolato nelle pagine che seguono) intorno alla differenza che passa tra il diritto e i diritti. Il diritto come insieme di norme presenti in un dato ordinamento giuridico (oggi dovremmo dire sempre più sovrannazionale), ma anche come giurisprudenza e scienza giuridica. I diritti in quanto facoltà concesse a ciascuno, in quanto risultato di ciò che è o non è permesso fare in relazione ad una determinata situazione, in quanto interessi dei singoli. Infine, in ordine all'ultima variabile si prendano in esame i mutamenti dei comportamenti anche sotto il versante antropologico, posto che l'uomo dell'era digitale è assai diverso dall'uomo dell'era analogica. E posto, altresì, che nel XX secolo il convincimento più diffuso ruotava intorno al principio in base al quale maggiore quantità d'informazione avrebbe determinato maggiore qualità della democrazia, mentre nel XXI secolo l'equazione da coltivare era (ed è) quella tra la qualità dell'informazione e la qualità della democrazia. In tale ottica può essere affrontata anche la questione dell'*infodemia*, enfatizzata dall'emergenza pandemica che, com'è noto, ha prodotto tre tipologie d'emergenza: sanitaria, economica, sociale.

Il libro ha il pregio di agevolare l'approfondimento di molti temi d'attualità, immaginandone una proiezione definita (ma non definitiva) nella sfera processuale e giurisdizionale. Sfera all'interno della quale si intrecciano questioni inerenti alle regole, alle sue violazioni e alle sanzioni giuridiche da comminare, senza tralasciare quelle sociali che si autodeterminano in base a valori, credenze, prassi e orientamenti. Alla base di questo obiettivo ermeneutico vi è anche la consapevolezza che i media possono essere considerati alternativamente o come tecnologie o come forme di comunicazione, vale a dire convenzioni e forme organizzate (Meyrowitz, 1985). Ciò vuol dire anche che essi, a partire dai social, vanno studiati in relazione al contesto: geografico, culturale, sociale, storico. I fenomeni della multimedialità e della crossmedialità, ma anche della convergenza culturale (Jenkins, 2006), che determina le tre tipologie di interattività (conversazionale, consultazionale, trasmissionale) sono anche da questo punto di vista elementi cruciali di dibattito. Del resto, sono queste le caratteristiche principali del Web 2.0, senza il quale i social network non avrebbero potuto svilupparsi. È questo il motivo per il quale le forme di comunicazione da prendere in considerazione, unitamente a quella *one-to-many,* sono le seguenti*: many-to-many*, *many-to-one*, *one-to-one.*

Tra le problematiche più interessanti presenti in questo libro, scritto a più mani e con uno stile divulgativo anche se non per questo meno approfondito, vi è quella delle *fake news*. Vale la pena di concentrarsi su questa evidenza empirica delle distorsioni, volontarie e involontarie, presenti nella società delle piattaforme.

Vanno messe in evidenza tre date. Nel 2013 il *Word Economic Forum* ha inserito la disinformazione tra i rischi globali del pianeta. Nel 2016 l'*Oxford Dictionary*

ha stabilito che la *key word* dovesse essere "*post-truth*". Nel 2017 il Consiglio d'Europa ha elaborato, infine, un rapporto intitolato *Information disorder*. In questo rapporto si prevedono sostanzialmente due tipologie applicative. La prima è quella della *disinformation*, ovvero la volontà di costruire notizie false per orientare comportamenti collettivi dopo aver modificato idee e opinioni individuali. La seconda è la *misinformation*, ovvero la diffusione involontaria di notizie false che si propagano in modo virale, indipendentemente dall'azione del produttore dei contenuti. È evidente che il discrimine tra la prima e la seconda tipologia risieda nella intenzionalità o meno dell'agire comunicativo habermasiano, quando e se esso sia effettivamente finalizzato alla proposizione nella sfera pubblica mediata, come la definisce Thompson, di elementi in grado di alterare la dinamica democratica o il funzionamento del mercato. Attenzione, però, perché la non intenzionalità, almeno nella produzione dell'effetto finale di manipolazione o parziale modificazione della realtà, è la chiave per leggere anche la distorsione involontaria presente nelle dinamiche di *newsmaking* sviluppate da parte dei cosiddetti *media mainstream*, ovvero stampa di massa, radio e televisione.

Fake news, *hate speech* e *deepfake* sono un effetto collaterale della orizzontalizzazione dei processi comunicativi, della prosumerizzazione frutto del ruolo interattivo e co-creativo nella generazione e diffusione dei contenuti da parte degli utenti (Giorgino, 2018). Viviamo in una società dis-intermediata o re-intermediata in cui assistiamo al primato dello *storytelling* rispetto a quelle forme di rappresentazione neutra della realtà. Una società atomizzata in cui, per dirla con Llyotard, le micro narrazioni individuali (di cui tutti siamo protagonisti sui social network) stanno gradualmente sostituendo le grandi narrazioni del XX secolo, cambiando anche la nostra concezione della "libertà": non libertà da noi stessi, come sarebbe giusto, ma libertà dagli altri. Siamo chiamati a governare non solo la dinamica polarizzante "verità-falsità", ma anche quella più subdola "verità-verosimiglianza", oppure "reale-realistico" o "fatti-fatti estesi" (Giorgino, 2020).

Agcom si è occupata del tema delle *fake news*, della percezione della realtà e delle sue ricadute sulla disinformazione. In Italia la gran parte della produzione di contenuti *fake* riguarda argomenti di politica e cronaca, mentre il resto riguarda soprattutto questioni di carattere scientifico. Più della metà degli italiani ha, inoltre, una falsa percezione di fenomeni misurabili in senso oggettivo e riguardanti diversi temi: economia, scienza ed ambiente, immigrazione, lavoro, criminalità. La diffusione di false percezioni può comportare come effetto indiretto anche la diminuzione della capacità di reazione dei cittadini davanti all'offerta di contenuti *fake*. Le "dispercezioni", si chiamano così nel gergo tecnico-scientifico, rendono infatti meno contrastabili i fenomeni di *disinformation* e *malinformation*.

Altro elemento di criticità dell'era dei social è il fenomeno delle *filter bubble* e delle *echo chamber* all'interno delle quali persone che condividono le stesse idee discutono tra loro e solo tra loro, acuendo così le problematiche connesse ad un'esposizione mediatica di tipo selettivo e di *confirmation bias*: scelgo ciò che mi conferma nell'opinione che ho maturato fino a quel momento.

Il premio Nobel per l'economia, lo psicologo Kahneman, ha invitato a distinguere tra il "pensiero veloce" e il "pensiero lento", sapendo che il primo, a differenza del secondo, si poggia su un basso impegno cognitivo e su risposte superficiali. L'individuo utilizza normalmente il primo sistema per far leva su dinamiche cognitive di tipo analogico-associativo, frutto cioè di pigrizia mentale. Utilizza il secondo sistema, ovvero il ragionamento, invece per avvalorare le proprie convinzioni e proteggere le proprie idee in un percorso logico-mentale di tipo "verificazionista", anziché "falsificazionista". Ad essere *fake* potrebbero perciò anche essere i nostri sistemi cognitivi, se non investiamo a sufficienza in pensiero critico, in progetti di *media education* nella doppia direzione di "educazione ai media" ed "educazione con i media". La prima opzione comporta il varo di investimenti in ordine alla creazione di una cultura del digitale, che è cosa ben diversa dall'acquisizione delle semplici competenze digitali. La seconda invece comporta la consapevolezza che, almeno per le giovani generazioni, il trasferimento della conoscenza avvenga (o possa avvenire) per il tramite anche di fonti informali.

Arriviamo così alla necessità di un cambio di paradigma in grado di recuperare le zone di contatto esistenti tra le ragioni della regolamentazione e quelle della formazione, tra le norme giuridiche e le condotte etiche. Il tutto in una logica di corresponsabilità tra produttori di contenuti, gestori delle piattaforme e fruitori. Questi ultimi sempre più interattivi (oltre che iperattivi) nella costruzione dei processi di significazione della realtà, in chiave denotativa e connotativa. Bene fa, dunque, la Fondazione Aiga a presidiare questi terreni esplorativi nei quali si può sperimentare l'intreccio esistente tra il diritto e la sociologia. Una conseguenza della strutturazione dell'ecosistema comunicativo digitale nella stagione dell'iper-connessione e dell'iper-complessità.

Capitolo 1
I social network

Francesco Colapaoli, Anna Coppola,
Francesca Romana Graziani, Mariarita Mirone

Sommario: 1. Definizione e inquadramento normativo. – 2. La convenzione di Budapest. – 3. Il Codice dell'Amministrazione Digitale. – 4. Il GDPR 2016/679.

1. Definizione e inquadramento normativo

L'Enciclopedia *on line* Treccani definisce *social network un servizio informatico on line che permette la realizzazione di reti sociali virtuali. Si tratta di siti internet o tecnologie che consentono agli utenti di condividere contenuti testuali, immagini, video e audio e di interagire tra loro. Generalmente i social network prevedono una registrazione mediante la creazione di un profilo personale protetto da password e la possibilità di effettuare ricerche nel database della struttura informatica per localizzare altri utenti e organizzarli in gruppi e liste di contatti* [1].

Questa definizione delinea quali sono le caratteristiche del *social network*, ovvero la realizzazione di una rete virtuale, la possibilità di condivisione dei contenuti, la possibilità di analizzare i contenuti altrui.

Già nel 2007, un importante approfondimento sul tema pubblicato sul *Journal of computer-mediated communication* a cura di due ricercatrici americane, Danah m. Boyd e Nicole B. Ellison, ha contribuito ad analizzare le ragioni di un fenomeno che in pochi anni avrebbe rivoluzionato la comunicazione [2].

In particolare, le due studiose hanno fornito una prima definizione: *We define social network sites as web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site.*

---

[1] V. *https://www.treccani.it/enciclopedia/social-network*.

[2] V. *https://academic.oup.com/jcmc/article/13/1/210/4583062.*

Dalla lettura di questo interessante approfondimento, si percepisce quanto già allora fosse chiaro che il fenomeno dei *social network* si sarebbe trasformato in un fenomeno globale che avrebbe in poco tempo modificato il nostro modo di comunicare e anche di interagire in un mondo, quello virtuale, potenzialmente senza confini e soprattutto, oggi lo possiamo affermare, sempre più interconnesso con il mondo reale, da intendersi nella sua dimensione fisica.

Infatti, la possibilità di rendere visibili e utilizzabili le proprie reti sociali costituisce il fulcro, il vero elemento distintivo del *social network* rispetto agli strumenti di mera comunicazione, ciò che evidentemente pone all'interprete una serie di questioni che, come vedremo, involgono la configurabilità di reati, con adattamenti necessitati da condotte nuove, nei limiti previsti dall'ordinamento giuridico, ma anche la necessità di introdurre i contenuti nel processo civile e nel processo penale a fini probatori, le stesse modalità di acquisizione della prova al fine di valutarne la genuinità e, non ultimo, questioni di *privacy*, visto che già nello studio appena citato si segnalava che *popular press coverage of social network sites has emphasized potential privacy concerns, primarily concerning the safety of younger users (George, 2006; Kornblum & Marklein, 2006). Researchers have investigated the potential threats to privacy associated with SNSs. In one of the first academic studies of privacy and SNSs, Gross and Acquisti (2005) analyzed 4,000 Carnegie Mellon University Facebook profiles and outlined the potential threats to privacy contained in the personal information included on the site by students, such as the potential ability to reconstruct users'social security numbers using information often found in profiles, such as hometown and date of birth.*

La proliferazione di piattaforme digitali, *social network*, semplici applicazioni costituite da software spesso molto sofisticati, con costante ed esponenziale implementazione delle possibilità di sfruttamento delle funzionalità, legate anche all'uso di algoritmi di intelligenza artificiale (con preoccupanti condizionamenti dei dibattiti come vedremo a proposito di *fake news* e infodemia), hanno determinato un aumento tuttora incalcolabile di utenti, ponendo sempre più frequentemente i legislatori di tutti i paesi di fronte a questioni e problematiche non sempre di semplice soluzione, anche in ambito processuale.

Il Legislatore italiano ha disciplinato questa complessa materia con diverse disposizioni di legge che, di seguito, senza pretesa di esaustività, essendo il quadro piuttosto articolato, si indicano: Codice per l'Amministrazione Digitale di cui al d.lgs. n. 82 del 2005 e relativo Regolamento allegato alla determinazione n. 160 del 17 maggio 2018 emanata dall'Agenzia per l'Italia Digitale presso la Presidenza del Consiglio dei Ministri, la legge 18 marzo 2008, n. 48, decreto Ministro della Giustizia n. 44 del 2011 e relative specifiche tecniche date con Provvedimento del Responsabile per i sistemi informativi automatizzati della Direzione Generale per i sistemi informativi automatizzati del 16 aprile 2014, Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, d.l. n. 179 del 2012, Regolamento Unione Europea 23 luglio 2014, n. 910, d.lgs. n. 70 del 2013 e il c.d. GDPR in materia di privacy, ovvero il Regolamento Europeo n. 679 del 2016.

Chiaramente, l'interprete che voglia approfondire la conoscenza specifica dei *social network* non può prescindere dall'esame delle disposizioni contenute nel c.d. Codice di Condotta europeo sottoscritto dalle piattaforme *Facebook*, *Google*, *Twitter*, *Mozilla*, più recentemente anche da *Microsoft* e *TikTok,* la dichiarazione dei diritti e delle responsabilità di Facebook, le regole di Twitter e le condizioni d'uso di Instagram, per restare nell'ambito dei *social network* più utilizzati in questo momento storico.

La ridda di disposizioni e la non secondaria circostanza che spesso gli ordinamenti giuridici disciplinano in modo completamente diverso l'utilizzo dei moderni strumenti di comunicazione pone all'interprete importanti sfide.

2. La Convenzione di Budapest

La legge 18 marzo 2008, n. 48, può essere considerata la risposta del legislatore italiano, all'esigenza di ottenere delle regole specifiche che fossero, perlomeno nelle intenzioni, idonee a garantire la conservazione e la genuinità del dato informatico [3].

Nonostante il progresso tecnologico ed il suo utilizzo all'interno del processo, necessitassero di un adeguamento normativo, il legislatore era rimasto sostanzialmente inerte.

Con la sottoscrizione della convenzione di Budapest del 2001, il legislatore internazionale, si muove proprio in questa direttrice apportando degli innesti, tanto di diritto sostanziale quanto di diritto processuale penale, con l'introduzione di plurime prescrizioni relative all'acquisizione della raccolta e conservazione delle prove digitali.

La convenzione si muove sostanzialmente su tre direttrici [4].

- definizione dell'ambito di applicazione delle misure processuali;
- previsione di misure per l'acquisizione dei dati informatici;
- previsione di misure coattive a ottenere i dati informatici.

L'ambito di applicazione del testo convenzionale è considerevole poiché esso si pone l'ambizioso obiettivo, di contrastare il cybercrime e di contrastare, i reati che in ogni caso vengono commessi attraverso l'utilizzo di un sistema informatico.

La novella ha introdotto delle modifiche ad ampio raggio, modificando l'art. 132 del Codice della privacy, ma incentrandosi prevalentemente su quegli innesti sostanziali e procedurali, utili, alla lotta ed alla repressione dei reati informatici.

Un ruolo preminente nel testo convenzionale, è rivestito dalla prova digitale, per

---

[3] G. RANALDI, *Processo penale e prova informatica: profili introduttivi*, in *Diritto Pubblico europeo online*, n. 2/2020.

[4] M.A. SENOR, *Convenzione di Budapest: le modifiche al c.p.p. ed al codice della privacy*, in *Altalex*, 20 maggio 2008.

la cui acquisizione, stante la sua ontologica fragilità, è predisposto un sistema di norme finalizzato a garantirne l'incorruttibilità.

Sebbene nelle intenzioni la normativa convenzionale si presentava, almeno in via potenziale, idonea a soddisfare le "esigenze processuali" poste dal progresso tecnologico, in sede di ratifica, tali aspettative sono state in parte disattese.

Per ciò che qui rileva, il legislatore nazionale si è limitato a prescrivere unicamente gli obbiettivi a cui deve improntarsi l'attività degli inquirenti, ovvero la preservazione del compendio probatorio digitale.

Ed infatti, in tal senso depone la disposizione inserita nel comma 2, dell'art. 244 c.p.p. impone che le attività di ispezione, vengano compiute con «*misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*».

Analogamente viene modificato anche l'art. 247 c.p.p. che al comma 1-*bis*, impone l'osservanza della medesima prescrizione, in occasione delle esecuzioni delle perquisizioni nei sistemi informatici.

Una ulteriore novità è rappresentata dall'intervento compiuto rispetto alla possibilità per gli inquirenti di procedere al sequestro di corrispondenza presso i fornitori di servizi postali telegrafiche telematici; come di pari rilievo è la modifica apportata all'art. 51 del codice di procedura penale.

Con particolare riferimento alle disposizioni innestate in ambito processuale, va segnalato che le stesse possono qualificarsi come delle *finalità* che si impongono all'autorità procedente, non essendo accompagnate da alcuna sanzione, nel caso di ricorso a tecniche investigative che potenzialmente possono minare la genuinità del dato.

In questo senso l'intervento normativo del 2008, può essere considerato incompleto, poiché di fatto, lascia libera l'autorità inquirente di individuare il protocollo investigativo più adatto.

Difatti, il risultato raccolto e la sua valenza probatoria, in assenza di una specifica sanzione che ne commini l'inutilizzabilità, è rimesso in ogni caso al libero apprezzamento del giudice [5].

3. Il Codice dell'Amministrazione Digitale

Il Codice dell'Amministrazione Digitale (per brevità, CAD) è stato adottato con il d,lgs. 7 marzo 2005, n. 82 e nasce dall'esigenza di riunire in un unico testo normativo le norme regolatrici dei rapporti tra pubblica amministrazione e privati (cittadini e imprese) in ambito di tecnologie dell'informazione e della comunicazione.

Il Codice è stato successivamente modificato e integrato con il d.lgs. 4 aprile

[5] Cass., Sez. V, 3 marzo 2017, in *Cass. Pen.*, 2017, 12, 446.

2006, n. 159, con il d.lgs. del 30 dicembre 2010, n. 235 con il d.lgs. 26 agosto 2016, n. 179 e, da ultimo, con il d.lgs. n. 217 del 13 dicembre 2017.

All'articolo 1, contiene, tra le altre, le definizioni di documento informatico, di documento analogico, di copia informatica di documento analogico, di copia per immagine su supporto informatico di documento analogico, di copia informatica di documento informatico, di duplicato informatico, di firma digitale, di identità digitale e si applica alle pubbliche amministrazioni, ai gestori di servizi pubblici, alle società a controllo pubblico, nonché ai privati ove non diversamente previsto [6].

Il CAD disciplina la validità e la efficacia probatoria dei documenti informatici, nonché delle copie informatiche dei documenti analogici e delle copie dei documenti informatici (analogiche e informatiche).

È stato il CAD, con l'art. 23-*quater*, a inserire all'art. 2712 c.c. dopo le parole "riproduzioni fotografiche" la parola "informatiche", dando di fatto (e di diritto) lo strumento giuridico per la disciplina dei Social Network nel processo civile.

Il CAD prevede, all'art. 71, l'adozione delle Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione del codice stesso (il cui rispetto, tra l'altro è requisito di validità del documento informatico).

Le regole tecniche – che fino ad oggi hanno trovato regolamentazione nel d.p.c.m. 3 dicembre 2013, contenente "Regole tecniche in materia di sistema di conservazione", nel d.p.c.m. 3 dicembre 2013 contenente "Regole tecniche per il protocollo informatico" e nel d.p.c.m. 13 novembre 2014, contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici" – sono, da ultimo, state aggiornate dalle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici", adottate dall'AgID [7] ed entrate in vigore dopo la pubblicazione sul relativo sito istituzionale [8], il 10 settembre 2020, ma con applicazione a partire dal duecentosettantesimo giorno successivo alla loro entrata in vigore e quindi dal 7 giugno 2021 [9].

A partire da tale data verranno abrogati il d.p.c.m. 3 dicembre 2013 contenente "Regole tecniche in materia di sistema di conservazione", il d.p.c.m. 13 novembre 2014, mentre il d.p.c.m. 3 dicembre 2013, contenente "Regole tecniche per il protocollo informatico" sarà solo parzialmente abrogato.

---

[6] Art. 2, comma 3, d.lgs. 7 marzo 2005, n. 82.

[7] L'Agenzia per l'Italia Digitale è l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica, istituita con il d.l. 22 giugno 2012, n. 83 convertito in legge 7 agosto 2012, n. 134.

[8] *https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_sul_documento_informatico_pdf.*

[9] La pubblicazione sul sito istituzionale di AgID è stata comunicata nella Gazzetta Ufficiale della Repubblica Italiana 19 ottobre 2020, n. 259.

Le regole tecniche emanate ai sensi dell'art. 71 del CAD, nel testo vigente prima dell'entrata in vigore del d.lgs. 13 dicembre 2017, n. 217, restano efficaci fino all'eventuale modifica o abrogazione da parte delle Linee guida, in conformità con quanto previsto dall'art. 65, comma 10 del d.lgs. n. 217/2017, come previsto dall'art. 8 del Regolamento per l'adozione di Linee Guida per l'attuazione del Codice dell'Amministrazione Digitale.

L'Unione Europea con il Regolamento n. 910 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno – c.d. Regolamento eIDAS (electronic IDentification Autenthication and Signature) – ha fornito inoltre una base normativa comune per interazioni elettroniche sicure tra i cittadini, le imprese e le Pubbliche Amministrazioni e ha valorizzato l'efficacia dei servizi elettronici e le transazioni commerciali elettroniche tra gli Stati membri.

Tale Regolamento, oltre a definire all'art. 3, n. 35) il documento elettronico e a riconoscerne espressamente efficacia giuridica (art. 46), sancisce all'articolo 25 il principio di non discriminazione della firma elettronica rispetto alla firma materiale (v. *infra*, cap. 5, par. 2.1).

4. Il GDPR 2016/679

Il Regolamento generale per la protezione dei dati personali n. 2016/679 (General Data Protection Regulation o GDPR) è la normativa europea in materia di protezione dei dati che, pubblicata nella Gazzetta Ufficiale Europea del 4 maggio 2016, è entrata in vigore il 25 maggio 2018, con abrogazione espressa della previgente Direttiva 95/46/CE.

Lo scopo del GDPR è stato quello di migliorare l'unitaria ed affettiva protezione dei dati personali, riconoscendosi che la preesistente normativa non ha sufficientemente impedito l'incertezza giuridica, avvertita dai cittadini, sul trattamento dei dati, specialmente su internet.

La direttiva, infatti, prendendo spunto dagli scambi commerciali in UE, concepiva staticamente la protezione dei dati come conseguenza del rapporto fra il titolare del trattamento e l'interessato favorendo la mera adozione di formalità (informative e consenso). Il dato personale era, quindi, assimilato ad un bene che non poteva essere utilizzato senza il consenso del suo "proprietario".

L'ottica cambia totalmente nel nuovo Regolamento UE poiché, con il crescente sviluppo economico-digitale, la protezione del dato personale non appare più sufficiente tramite lo strumento del consenso ma, più profondamente, attraverso uno stratificato controllo del dato, così da renderlo compatibile con la sua libera (legittima) circolazione.

Ecco che, infatti, il dato non è più protetto dal consenso e dagli altri presupposti del trattamento ma, anche e soprattutto, dall'imposizione a carico del titolare del trattamento di specifici obblighi di "auto-responsabilizzazione". Oggi, infatti, il ti-

tolare del trattamento, per garantire l'idoneità dei propri processi di trattamento, dovrà anche impegnarsi ad adottare tutte quelle misure tecniche ed organizzative sufficienti a garantire un livello di sicurezza adeguato al rischio.

Dal concetto formale del trattamento basato sul consenso si è, quindi, passati, a quello sostanziale di accountability del titolare del trattamento che, oltre alle regole generali del GDPR, dovrà orientarsi autonomamente nel decidere il "miglior tipo di trattamento dei dati personali".

La riforma comunitaria ha comportato, poi, l'inevitabile novella, a livello nazionale, del Codice della privacy (d.lgs. 30 giugno 2003, n. 196) attraverso il d.lgs. 10 agosto 2018, n. 101, entrato in vigore il 19 settembre 2018, con il quale sono state abrogate tutte le norme del nostro Codice della privacy risultate incompatibili con il Regolamento UE n. 2016/679 ed introdotte nuove disposizioni ad esso conformi.

Capitolo 2

Fake news *e reati*

Francesco Colapaoli

Sommario: 1. *Fake news* e *infodemia*. Brevi cenni di analisi di un fenomeno in costante evoluzione. – 2. Pubblicazione di notizie false, esagerate o tendenziose atte a turbare l'ordine pubblico (art. 656 c.p.). – 3. Procurato allarme presso l'Autorità (art. 658 c.p.) e abuso della credulità popolare (art. 661 c.p.). – 4. Rialzo e ribasso fraudolento di prezzi sul pubblico mercato o nelle borse di commercio (art. 501, comma 1, c.p.).

1. *Fake news* e *infodemia*. Brevi cenni di analisi di un fenomeno in costante evoluzione

Negli ultimi anni, il tema delle *fake news* è divenuto centrale nel dibattito politico, stante i non secondari effetti distorsivi che la diffusione di notizie false può comportare nel corso dei procedimenti elettorali, ma anche per quelli che possono investire il mondo dell'informazione, con preoccupanti risvolti che coinvolgono la collettività, proprio per la rapidità e per la capillarità della diffusione dovuta all'utilizzo di strumenti informatici.

Infatti, come vedremo, in tempi recenti è stata promossa un'opera di sensibilizzazione che, coinvolgendo diverse categorie di operatori, si propone l'ambizioso fine di contrastare il fenomeno della proliferazione delle *fake news.*

Volendo fornire una definizione, generalmente si parla di *fake news* facendo riferimento a notizie sostanzialmente false supportate da dati inesistenti e fatti inventati, le quali vengono veicolate utilizzando fonti che, ad un'analisi concreta, si rivelano sempre completamente inattendibili.

Più specificamente, la virulenza che caratterizza la diffusione delle cosiddette bufale, si deve spesso al fenomeno del c.d. *click baiting*, ovvero la pubblicazione di notizie false con titoli sensazionalistici e foto che inducono l'ignaro internauta a cliccare, generando un guadagno per il gestore del sito web, legato ad introiti di natura pubblicitaria.

Sempre con riferimento al *click baiting* un altro effetto particolarmente dannoso è la diffusione di c.d. *malware*, ovvero software che si autoinstallano sui computer

degli utenti mettendone a rischio il funzionamento ovvero eliminandone i dati, il tutto al fine di procurare profitti illeciti, con conseguente danno per tutti gli utenti.

Un'altra modalità di diffusione delle *fake news*, le quali generano una manipolazione artificiale della realtà fattuale, non poteva che essere affidata a profili di utenti *social* parimenti artificiali, siccome generati da specifici software che hanno come unico fine quello di simulare e rilanciare conversazioni – finte – tra persone realmente non esistenti.

Si tratta dei c.d. *bot* (abbreviazione di *robot*) ovvero algoritmi di intelligenza artificiale in grado di dialogare con gli utenti, che sono piuttosto comuni in ambito commerciale perché sui siti internet si sostituiscono agli esseri umani rispondendo in maniera automatica a domande predefinite.

Viceversa, sempre più spesso, nell'ambito dei *social network* (si parla al riguardo di *social bot*) questi profili artificiali vengono utilizzati per simulare conversazioni tra esseri umani ovvero, nel caso di altre applicazioni, come Instagram o Twitter, per simulare un numero elevato di c.d. *follower* o per rilanciare rapidamente determinati messaggi.

La diffusione di questi profili *social* completamente fittizi, ha subito un grandissimo incremento con pesantissime ricadute sulla veicolazione incontrollata di *fake news* che, soprattutto in ambito politico, sono sempre più sfruttate per condizionare le opinioni o per focalizzare artatamente l'attenzione su determinati eventi, a soli fini distorsivi sull'opinione pubblica.

Tale preoccupante fenomeno sembra particolarmente agevolato anche dal funzionamento degli algoritmi che sono alla base del funzionamento dei *social network* i quali per ragioni squisitamente tecniche a volte favoriscono la diffusione di notizie generate dai *social bot*, con ciò determinandosi un pericoloso effetto gregge in grado di condizionare e orientare le scelte degli utenti e quindi le dinamiche sociali.

Al fine di contrastare il fenomeno della diffusione delle c.d. bufale, sono nate specifiche figure professionali come il *debunker*, ovvero il demistificatore o disingannatore, rappresentato da un professionista, ovvero una organizzazione, deputati specificamente ad individuare le notizie false, mentre più recentemente, si sono moltiplicate, a livello internazionale e anche nel nostro Paese, siti internet che si occupano di *fact-checking* [1], ovvero verifica dei fatti monitorando la diffusione di notizie false e fornendo un servizio di informazione che consenta ai cittadini di verificare la genuinità e la fonte delle notizie, orientandosi consapevolmente nella ridda di dati messi a disposizione dal web.

Tuttavia, nonostante l'opera di sensibilizzazione messa in campo negli ultimi anni, il problema ha assunto una connotazione diversa e una dimensione planetaria dall'inizio del 2020, a seguito della diffusione incontrollata di notizie generata dall'emergenza sanitaria legata all'infezione da coronavirus.

---

[1] V. *https://www.agcom.it/siti-di-fact-checking+&cd=4&hl=it&ct=clnk&gl=it*.