Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019), pp. 11-28

Deepfake, ovvero *Manipola et impera*. Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda

Federica Bertoni*

Sommario: 1. Breve premessa al tema. – 2. Origine e natura dei deepfake. – 3. I bìas di conferma e le profondità del falso. – 3.1. La profondità relativa al grado di realismo dei deepfake: la tecnologia e le tecniche sottostanti. – 3.2. La profondità delle identità e degli intenti di chi realizza o commissiona deepfake e la "questione fonti". – 3.3. La profondità del livello d'impatto politico e sociale: alcuni esempi di deepfake. – 4. La necessità di una definizione condivisa. – 5. "Deepfake app" e diffusione: un problema di democrazia al contrario. – 6. Falso profondo: i metodi e gli strumenti tecnici d'individuazione e contrasto. – 7. Considerazioni conclusive.

1. *Breve premessa al tema*

Le fake news digitali non rappresentano più una novità, tant'è che sul finire del 2017 il Collins Dictionary ha eletto l'espressione "fake

* Informatico Forense, certificata CIFI, è Perito e Consulente Tecnico presso il Tribunale Ordinario di Brescia. Laureata alla Facoltà di Giurisprudenza dell'Università degli Studi di Brescia con una tesi in Informatica Giuridica incentrata sugli aspetti di sicurezza informatica e giuridici del fenomeno del "phishing", è stata fra i primi in Italia ad occuparsi di Digital Forensics. È stata Conciliatore presso il Servizio di Conciliazione e Arbitrato presso la CCIAA di Brescia, in controversie in materia di telecomunicazioni. Presta la propria consulenza a studi legali, aziende, Procure e Forze dell'Ordine nel settore dei cybercrime, nel significato più ampio del termine. È membro del Capitolo italiano di IISFA ed è socia e docente CLUSIT. Dal 2003 è autrice e coautrice di diverse pubblicazioni in materia di Sicurezza informatica, Diritto dell'Informatica e delle Nuove Tecnologie e Informatica Forense. Collabora con le Cattedre d'Informatica Giuridica delle Facoltà di Giurisprudenza dell'Università degli Studi di Brescia e Pavia. È Affiliate Scholar dell›Information Society Law Center presso l'Università degli Studi di Milano.

news" quale "parola dell'anno", attribuendole la seguente definizione: «false, often sensational, information disseminated under the guise of news reporting»[1]; al contempo, negli ultimi anni, gli sforzi tesi a potenziare e a fortificare negli utenti le capacità di attenzione e reazione alle bufale online, non si sono di certo fatti attendere. Basti pensare all'opera di sensibilizzazione verso il problema delle fake news attuata dalle stesse piattaforme social per il tramite del cosiddetto *fact-checking*, che, da semplice forma d'incoraggiamento iniziale, fattosi via via più pressante nonché severo nei toni e rivolto agli utenti affinché si assumessero una parte di responsabilità all'interno del processo di verifica della veridicità delle notizie, prima di postarle e farle circolare in rete, ha finito col trasformarsi nella predisposizione di strumenti tecnici, che gli stessi social network dovrebbero utilizzare, col supporto delle segnalazioni degli utenti, per rendere più agevoli, rapidi e razionalizzati i controlli sulle fake news[2]. Le necessità appena evidenziate scaturiscono dal fatto che, come puntualmente osservato da Walter Quattrociocchi, «l'essere umano non è razionale, come ci ostiniamo a credere, bensì ha una visione del mondo che è emotiva e percettiva»[3].

A quanto appena sottolineato si deve aggiungere una notazione ulteriore e fondamentale per inquadrare l'argomento dei deepfake in maniera utile e cioè che, come l'esperienza insegna, la tecnologia non solo non ha mai atteso che il suo demiurgo la perfezionasse, aggiustandola dove necessario, ma addirittura ha sempre battuto in velocità l'uomo, mettendolo di volta in volta con le spalle al muro, attraverso sfide che egli non aveva saputo prevedere, in maniera opportuna, col giusto grado di anticipo, lasciandolo, di fatto e nelle immediatezze, sguarnito di qualsivoglia tipo di protezione. Il progresso tecnologico, che con l'intelligenza artificiale ha già compiuto il tanto sospirato quanto temuto balzo in avanti, prosegue inesorabile il proprio cammino e avanza, senza peraltro mutare nei modi che più la caratterizzano: mentre reca con sé indubbi vantag-

[1] Collins English Dictionary, *Definition of "fake news",* disponibile in Internet al seguente indirizzo: https://www.collinsdictionary.com/dictionary/english/fake-news.

[2] Si veda, al riguardo, la pagina "Fact-checking indipendente su Facebook", disponibile in Internet all'indirizzo https://www.facebook.com/help/publisher/182222309230722.

[3] Cfr. G. Bona, "Walter Quattrociocchi: come ti prevedo le fake news", in *Scienza in Rete*, in Internet all'indirizzo https://www.scienzainrete.it/articolo/walter-quattrociocchi-come-ti-prevedo-le-fake-news/giulia-bona/2018-04-03.

Deepfake, ovvero Manipola et impera*. Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda*

I deepfake rappresentano il nuovo cancro dell'informazione on line. Sono fake d'acciao, nate dalla costola di alcune tecniche che l'intelligenza artificiale sottintende. I deepfake plasmano il mondo del verosimile in una maniera tanto sofisticata da cancellare i confini fra ciò che è vero e ciò che è falso, fino a forgiare una seconda realtà, parallela alla prima. I deepfake sono profondi nel loro grado di realismo e nelle intenzioni di chi li produce, ma sono profondi, soprattutto, nel grado d'impatto politico e sociale che possono raggiungere. Considerati alla stregua di potenziali armi cibernetiche sfruttabili contemporaneamente su tutti i piani su cui poggia oggi la nostra esistenza, i deepfake debbono essere attentamente monitorati e studiati; nondimeno un'accurata analisi condotta su di essi potrebbe svelare tutti gli elementi utili per disegnare le linee guida essenziali ai fini della loro corretta gestione, nell'ottica della fisiologica trasversalità del problema tecnologico-giuridico che incarnano.

Deepfake, ovvero Manipola et impera*. Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda*

The deepfake represent the new cancer of information online. They are steel fake, born from the rib of some techniques that the AI implies. The deepfake shape the world of plausible in a way so sophisticated to erase the boundaries between what is true and what is false, to forge a second reality, parallel to the first. The deepfake are deep in their degree of realism and the intent of those who produce them, but they are deep, especially in the degree of political and social impact that can reach. Treated as potential cybernetic weapons exploitable simultaneously on all floors on which our existence is based, the deepfake must be closely monitored and studied; nevertheless, a careful analysis conducted on them might reveal all relevant information required to draw the essential guidelines for their proper management, with a view of physiological trasversality of the technological and legal problem that they embody.

Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019), pp. 29-42

La gestione individuale e collettiva del diritto d'autore alla luce del recepimento della Direttiva 2014/26/UE

Deborah De Angelis*

Sommario: 1. Introduzione. – 2. Libertà di scelta vs monopolio. – 3. L'evoluzione del sistema di gestione individuale dei diritti d'autore attraverso l'uso delle licenze Creative Commons.

1. *Introduzione*

L'intento della presente trattazione è quello di mettere in luce come, negli ultimi dieci anni, grazie all'evoluzione delle forme di sfruttamento economico delle opere dell'ingegno in formato digitale e all'affermarsi dell'utilizzo delle licenze di diritto d'autore con alcuni diritti riservati, la facoltà di gestione individuale del diritto d'autore si sia esponenzialmente affermata nel mercato delle opere dell'ingegno, in alternativa alla gestione collettiva.

In Italia, ove per oltre un secolo la gestione collettiva del diritto d'autore è stata caratterizzata da un regime di monopolio esclusivo, attribuito per legge alla Società Italiana degli Autori ed Editori (di seguito, per brevità, SIAE), non si era sentita sinora l'esigenza di discutere dell'effettivo esercizio della «facoltà spettante all'autore, ai suoi successori o agli aventi causa, di esercitare direttamente i diritti loro riconosciuti», lasciata impregiudicata dalla Legge 22 aprile 1941, n. 633[1] (di seguito, per brevità, L.d.A.).

La dottrina e la giurisprudenza, per ovvie e preminenti ragioni di tutela di un mercato – come quello della intermediazione dei diritti d'autore – caratterizzato da una posizione di monopolio degli organismi pubblici o privati che, per legge o di fatto, agivano in posizione dominante[2],

* Avvocato in Roma.

[1] Cfr. art. 180, comma 4, L.d.A.

[2] Si è sempre ritenuto che, nonostante la legge consenta la facoltà di esercizio diretto dei diritti d'autore, l'estesa diffusione delle opere dell'ingegno (soprattutto con riferi-

si sono maggiormente concentrate sulle questioni concernenti l'applicazione del diritto antitrust.

Ciò nonostante, come premesso, la facoltà degli autori di esercitare direttamente i loro diritti d'autore, in alternativa alla gestione collettiva, ha avuto un grande slancio, grazie all'utilizzo delle licenze di diritto d'autore, le cosiddette "Licenze Creative Commons", soprattutto nel settore dell'esecuzione della musica di sottofondo nei pubblici esercizi.

In tale scenario, sviluppatosi in costanza del regime di monopolio esclusivo, la SIAE ha dovuto prendere atto dell'evoluzione di un mercato parallelo, costituito dallo sfruttamento economico di repertori musicali gestiti direttamente dai titolari, e – di fatto – non lo ha ostacolato.

La Direttiva 2014/26/UE sulla gestione collettiva dei diritti d'autore e dei diritti connessi e sulla concessione di licenze multi-territoriali per i diritti su opere musicali per l'uso on line nel mercato interno (in breve, di seguito, "Direttiva Barnier")[3] ha spinto gli Stati membri ad adottare un processo volto alla liberalizzazione dell'attività di intermediazione dei diritti d'autore, riconoscendo all'autore la libertà di scelta dell'organismo di gestione collettiva (o dell'entità di gestione indipendente) a cui affidare le proprie opere[4].

La Direttiva Barnier propone di migliorare il funzionamento di tali enti attraverso la garanzia di elevati standard in materia di *governance*, gestione finanziaria, trasparenza e comunicazioni e di coordinare la normativa degli Stati membri circa la concessione di licenze multi-territoriali per i diritti sulle opere musicali online, in un settore ove l'attività di intermediazione collettiva dei diritti digitali non ha ancora raggiunto l'efficienza richiesta per garantire un buon livello di tutela e un'adeguata remunerazione per gli aventi diritto.

mento alla comunicazione al pubblico delle opere musicali) abbia comportato sempre l'esigenza dell'attività di intermediazione della SIAE (Corte cost. 90/241, F. it. 90, I, 2401, nota Nivarra); Commento all'art. 180, L.C. Ubertazzi, in *Commentario breve alle leggi sulla proprietà intellettuale e concorrenza*, X.B, 511. Ovviamente, l'ambito di applicazione della suddetto disposto normativo attiene alla gestione del diritto patrimoniale d'autore, come eccezione alla regola della gestione collettiva. Per la tutela del diritto morale d'autore, invece, vale la regola della gestione individuale.

[3] Direttiva 2014/26/UE del Parlamento Europeo e del Consiglio del 26 febbraio 2016, in Gazzetta ufficiale dell'Unione europea L. 84/72 del 30.3.2014.

[4] Cfr. art. 5 della Direttiva.

La gestione individuale e collettiva del diritto d'autore alla luce del recepimento della Direttiva 2014/26/UE

L'evoluzione delle forme di sfruttamento delle opere digitali e l'affermarsi dell'utilizzo delle licenze di diritto d'autore con alcuni diritti riservati, come strumento di condivisione delle opere dell'ingegno in rete, ha contribuito a facilitare l'esercizio individuale del diritto d'autore da parte dei titolari dei diritti. Tale facoltà non aveva mai avuto una concreta applicazione, seppure prevista già dalla Legge n. 633/1941.

La gestione individuale e collettiva del diritto d'autore alla luce del recepimento della Direttiva 2014/26/UE

With the evolution of digital copyright exploitation and the emergence of the use of copyright licenses with some reserved rights, as a way of for sharing artworks online, has helped to facilitate the individual exercise of the copyright by the copyright-holders. This power has never had a concrete application, although already provided for by Law no. 633/1941.

Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019), pp. 43-64

Profili giuridici delle valute virtuali

Carlo Lanfranchi*

Sommario: 1. Introduzione. – 2. Le valute virtuali come beni. – 3. La *blockchain* come contratto normativo. – 4. Meritevolezza del contratto e meritevolezza del bene. – 5. Le valute virtuali come bene "ambiguo". – 6. Le valute virtuali come bene "precario". – 7. Le valute virtuali come documento informatico rappresentativo di un contratto atipico. – 8. Conclusioni.

1. *Introduzione*

La qualificazione giuridica delle valute virtuali sconta, da un lato, la varietà delle loro declinazioni e, quindi, la difficoltà di descrivere sinteticamente un fenomeno relativamente nuovo e certamente complesso[1] e, dall'altro, la frammentarietà del loro riconoscimento legislativo e, quindi, l'impossibilità di dare a quest'ultimo una compiuta sistematizzazione. La natura giuridica delle valute virtuali pare, infatti, sfuggire alle categorie del diritto finanziario, provando a collocarsi – allo stadio attuale della legislazione – in quelle – residuali e generali – del diritto civile. Se, infatti, le nozioni di moneta avente corso legale e moneta elettronica, di titolo di credito tipico, di strumento finanziario, di prodotto finanziario e – quanto al profilo dell'attività – di servizio di pagamento paiono incapaci di inquadrare giuridicamente il fenomeno nei suoi tratti tipizzanti e fisiologici, nel tentativo di esaurire le categorie giuridiche "obiettive", dev'esserne provata – per completezza – la più essenziale: quella di "bene".

2. *Le valute virtuali come beni*

La categoria dei beni giuridici è rappresentata, secondo la definizione che ne dà il legislatore italiano, dalle «cose che possono formare oggetto di diritti»[2]. Si tratta, allora, di chiarire se le valute virtuali possano dir-

* Dottore di ricerca in Diritto commerciale. Le opinioni espresse sono personali e non impegnano in alcun modo l'Istituzione di appartenenza.

[1] Per questa ragione, si farà, qui, riferimento – pressoché esclusivo – alle valute virtuali del genere Bitcoin.

[2] Cfr. art. 810 c.c.

si, anzitutto, «cose» (*sub specie* di cose materiali (*res*) o, perlomeno, di entità immateriali[3]) in senso giuridico.

Al riguardo, paiono potersi ricavare dal dibattito dottrinale, formatosi attorno alla norma citata, tre nozioni alternative di "cosa" in senso giuridico, e, quindi, di "bene":

i) la cosa come entità oggetto di appropriazione[4];

ii) la cosa come entità che ha un valore di scambio[5] o un valore d'uso[6];

iii) la cosa come entità meritevole di tutela da parte dell'ordinamento[7].

Le valute virtuali – come si dirà – paiono suscettibili di "mimare" ciascuna delle tre nozioni richiamate e desumibili dalle disposizioni del codice civile ma, allo stesso tempo, soltanto in modo instabile. Sono – si potrebbe dire – beni "precari". D'altra parte, essi ricavano la propria ragion d'essere non da un dato di natura o di diritto a loro intrinseco, bensì da un accordo privatistico, istitutivo di un protocollo di funzionamento: la c.d. *blockchain*. Potrebbero essere, in questo senso, qualificati anche come beni "di secondo grado"[8], beni, cioè, che assumono la loro essenziale qualità solo all'interno e in ragione del proprio contesto di riferimento, il quale, allora, acquisisce carattere "ordinamentale", definendo i beni medesimi e i criteri di attribuzione della loro titolarità. Si afferma, così, – in qualche misura[9] – un'inversione logica nel rapporto tra beni e "accordi". Le valute virtuali, infatti, – per definizione – non preesistono all'accordo che le istituisce, risultando inseparabili dal proprio sottostan-

[3] Secondo alcuni, ad es., il c.d. *know-how*; ma, come si vedrà, in forza pur sempre – in quanto bene immateriale – di un intervento del legislatore.

[4] Cfr. F. Santoro Passarelli, *Dottrine generali di diritto civile*, Napoli, Jovene editore, 1999.

[5] Cfr. P. Barcellona, *Diritto privato e società moderna*, Napoli, Jovene editore, 1996.

[6] Cfr. A. Jannarelli, *La disciplina dei beni tra proprietà e impresa nel codice del 1942*, in AA.VV., *Letture di diritto privato*, Bari, 1994.

[7] Cfr. M. Costantino, "I beni in generale", in *Trattato di diritto privato*, diretto da P. Rescigno, vol. VII, Torino, 1982.

[8] Il richiamo è, evidentemente, alle azioni («la partecipazione sociale è rappresentata da azioni» art. 2346 c.c.), di cui non a caso è discussa la natura giuridica: se siano, cioè, pienamente qualificabili come titoli di credito. Esse, però, sono per certo, a differenza dei bitcoin, documenti nominati dalla legge, la quale, ad esempio e soprattutto, ne disciplina, almeno in via suppletiva, le modalità di circolazione.

[9] La *consecutio* logica pare la seguente: un bene giuridico immateriale (la tecnologia *blockchain*) è alla base di un accordo (la tenuta di un registro contabile) che "crea" un nuovo bene (la valuta virtuale) che ha natura elettronica e fonte contrattuale.

Profili giuridici delle valute virtuali

Il saggio studia i profili giuridici delle valute virtuali definite da un protocollo Bitcoin. Rilevata l'incapacità delle attuali categorie del diritto finanziario a contenerne la fattispecie, il fenomeno è stato misurato sulle categorie generali del diritto civile: dapprima, quella di bene giuridico ed, infine, quella di contratto. Distinto il protocollo (*blockchain*) dal suo veicolo (bitcoin), si è proposta la qualificazione del primo in termini contrattuali/ordinamentali e la qualificazione del secondo in termini di documento di legittimazione. Il contratto istitutivo del protocollo, ricondotto al genere del contratto normativo atipico, è stato, quindi, analizzato, sia dal punto di vista della *governance* dell'organizzazione che esso fonda, sia dal punto di vista della "meritevolezza di tutela" degli interessi che esso è diretto a realizzare. Da un lato, ne è stata rilevata la natura volontaristica e la forte dipendenza dalle aspettative degli agenti economici, e, di conseguenza, l'intima fragilità, dall'altro, la propensione a svolgere funzioni di rango pubblicistico e la difficoltà di *enforcement*, e, perciò, la potenziale "immeritevolezza". In conclusione, si sono tratte dall'analisi svolta tre opzioni di *policy*: i) riconoscere il protocollo quale ordinamento privato, ii) dichiarare l'inefficacia del contratto istitutivo in quanto "immeritevole", iii) integrare lo schema di protocollo nell'ordinamento statuale.

A legal examination of Bitcoin

This paper investigates the legal nature of crypto-assets based on a Bitcoin blockchain under the Italian law. Firstly, it suggests to distinguish blockchain (the protocol) from bitcoin (the vehicle). Secondly, it argues that bitcoin is an electronic document representing a "regulatory" contract. This contract creates a private legal framework, alternative, at least partially, to States' legal frameworks, that aims to verify digital events.

Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019), pp. 65-116

Attività amministrativa e intelligenza artificiale

Luigi Viola*

Sommario: 1. L'atto amministrativo ad elaborazione elettronica: un processo di (progressiva) trasformazione. – 2. Il cavallo di Troia per la penetrazione dell'I.A. nella sistematica amministrativa: la limitazione agli atti vincolati. – 2.1. La costruzione del sistema: l'inserimento del programma informatico nella sistematica amministrativa. – 2.2. Gli altri aspetti della teorica dell'atto amministrativo ad elaborazione elettronica: in particolare, partecipazione, motivazione e teorica dell'invalidità. – 2.3. Le responsabilità. – 3. Limiti e possibilità dell'aggancio all'attività amministrativa vincolata: i mobili confini dell'atto vincolato. – 3.1. Il legame con la teoria dell'autolimite della p.a. – 3.2. L'estensione all'ambito processuale. – 3.3. Le teorie a "corto raggio": in particolare, l'automazione per fasi e l'estensione alla discrezionalità tecnica. – 3.4. L'estensione ai territori della discrezionalità e la necessità di un cambio di prospettiva. – 4. Dalla sostituzione alla simbiosi: l'interazione uomo-sistema informatico.

1. *L'atto amministrativo ad elaborazione elettronica: un processo di (progressiva) trasformazione*

Come in qualsiasi altro campo dell'attività umana, anche l'attività amministrativa ha subito, negli ultimi decenni, significative trasformazioni derivanti dal sempre più massiccio ricorso alle nuove tecnologie in generale e all'informatica e alla telematica, in particolare; l'impatto delle nuove tecnologie sull'attività amministrativa ha poi dato vita a diverse "combinazioni" dei due diversi mondi che vanno dall'utilizzazione del computer con funzioni di *word processor* o *database* (soluzione, in un certo senso, minimale e che non modifica, se non indirettamente, le categorie sedimentate del diritto amministrativo) ai cd. atti amministrativi *in*

* Consigliere T.A.R Toscana e professore a contratto di diritto sportivo nell'Università degli Studi di Udine.

forma elettronica in cui la determinazione amministrativa è, non solo elaborata, ma anche formalizzata in forma elettronica e su supporto digitale.

Il riferimento già operato nel titolo all'intelligenza artificiale (di seguito indicata anche come I.A.) evidenzia però come l'oggetto del presente scritto sia la combinazione di informatica e attività amministrativa, in un certo senso, più avanzata, spesso definita come atto amministrativo *ad elaborazione elettronica* e riferita alle ipotesi in cui «è il computer a predisporne il contenuto, con tutte le implicazioni che ne derivano in ordine allo studio dei relativi elementi, delle connesse patologie e degli strumenti di tutela giurisdizionale»[1]; in questo caso, è quindi lo stesso computer a «definire […] – in base ad un *input* e ad un programma – il contenuto di un regolamento di interessi; può produrre esso stesso atti amministrativi»[2].

Del resto, si tratta di un processo che può essere descritto anche in maniera decisamente più plastica ed evocativa; si veda, ad esempio, la rilevazione relativa al "salto di qualità" derivante «dal passaggio dalla fase del "computer-archivio" alla fase del "computer-funzionario"» spesso operata da Alfonso Masucci[3] o il riferimento al passaggio dalle «"appli-

[1] La definizione è di F. Saitta, "Le patologie dell'atto amministrativo elettronico e il sindacato del giudice amministrativo", in «Rivista di diritto amministrativo elettronico», www.cesda.it, 2003, p. 2; «Dir. economia», 2003, p. 615. A p. 1 dello scritto, Saitta inserisce nella definizione anche l'ulteriore precisazione relativa all'elaborazione dell'atto "senza apporto umano"; come sarà precisato al § 4, la limitazione in questione appare però, oltre che fuorviante, contraria ad alcune limitazioni derivanti dal diritto positivo e in particolare, dalla normativa in materia di *privacy*; una definizione sostanzialmente analoga è utilizzata da A.G. Orofino, "La patologia dell'atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela", *Foro amministrativo - Cons. Stato*, 2002, p. 2256; Giur. merito, 2003, p. 400.

[2] Cfr. A. Masucci, "Atto amministrativo informatico", *Enciclopedia del diritto*, Milano, Giuffrè, 1997 Aggiorn. vol. I, 221, § 1; sostanzialmente non dissimile è la definizione di atto amministrativo automatico di G. Duni, *L'amministrazione digitale. Il diritto amministrativo nella evoluzione telematica*, Milano, Giuffrè, 2008, p. 74; Id. *Teleamministrazione*, Encicl. giur. Treccani, Roma, voce aggiornata 2007, vol. XVI, p. 5; a dimostrazione della sostanziale interscambiabilità delle definizioni di atto amministrativo ad elaborazione elettronica e atto amministrativo automatico, P. Otranto, *Decisione amministrativa e digitalizzazione della p.a.*, www.federalismi.it, 2018, 2, p. 15 le utilizza entrambe.

[3] Cfr. A. Masucci, *L'atto amministrativo informatico. Primi lineamenti di una ricostruzione,* Napoli, Jovene, 1993, p. 13 e Id. *Atto amministrativo informatico,* cit., § 1 che cita, al proposito, J. Frayssinet, *La bureaucratique: l'administration française face à l'informatique*, Paris, Berger-Levrault, 1981, p. 15; la definizione francese di *bureaucratique,*

Attività amministrativa e intelligenza artificiale

Lo scritto analizza le problematiche relative all'automazione del procedimento di emanazione degli atti amministrativi nell'ordinamento italiano, pacificamente ammessa con riferimento agli atti ad emanazione vincolata. Vengono, in particolare, analizzate le diverse problematiche relative all'inserimento del programma informatico nella sequenza di emanazione dell'atto amministrativo ed alla possibilità di attribuire al programma un ruolo completamente sostitutivo dell'intervento del pubblico funzionario.

Attività amministrativa e intelligenza artificiale

The paper analyzes the problems related to the automation of the procedure for the formation of administrative acts in the Italian legal system, peacefully admitted with reference to the restricted acts. In particular, the problems related to the insertion of the computer program in the sequence of formation of the administrative act and to the possibility of attributing to the program a role completely replacing the intervention of the public official are analyzed.

Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019), pp. 117-129

Il consumatore nella prospettiva dei *big data*: alcune considerazioni filosofico-giuridiche

Adriano Zambon*

Sommario: 1. I *big data* e il concetto di consumatore. – 2. Tre immagini scientifiche del consumatore. – 3. Conseguenze sul diritto: il modello di consenso nel GDPR. – 4. Considerazioni conclusive.

1. *I* big data *e il concetto di consumatore*

Il recente diritto dei consumatori è indubitabilmente influenzato dall'espansione dei cosiddetti *big data*. Quest'ultima espressione è ambigua, perché viene usata per designare sia delle particolari entità sia, per estensione, un insieme di attività che hanno ad oggetto tali entità. Le entità in questione sono contraddistinte da due caratteristiche: una caratteristica qualitativa, per cui sono dei dati; una caratteristica quantitativa, per cui sono, genericamente parlando, presenti in grande quantità. La seconda caratteristica, ovviamente, è una proprietà relativa: l'abbondanza dei dati a cui ci stiamo riferendo è parametrata sull'abbondanza dei dati che potevano essere raccolti dagli esseri umani in passato, più precisamente in periodi antecedenti alla cosiddetta rivoluzione digitale; confrontando la quantità di dati disponibili in tali periodi con la quantità di dati che possono essere raccolti oggi, possiamo qualificare i secondi come "*big*". Anche le attività che hanno ad oggetto questi ultimi, come si è detto, possono essere designate dall'espressione '*big data*'. Le attività in questione, più precisamente, consistono, in generale, nell'analisi dei *big data* (nella prima delle due accezioni) rivolta a fini predittivi e realizzabile grazie all'intersezione di informatica e statistica. Dal momento che i dati in

* Università degli Studi di Milano, Dipartimento di Scienze giuridiche "Cesare Beccaria", Sezione di Filosofia e Sociologia del diritto. Desidero ringraziare i partecipanti alla *Digital Transformation Law Conference*, tenutasi presso l'Università degli Studi di Milano tra il 12 e il 14 dicembre 2018, per i commenti a una versione precedente di questo testo.

questione e, di conseguenza, la loro analisi possono avere ad oggetto il comportamento dei consumatori, il diritto dei consumatori, come si è notato, non può non esserne influenzato.

Questa influenza può essere colta se si pone attenzione al modo in cui i *big data* plasmano una precisa immagine del consumatore. L'immagine in questione, data la sua dipendenza da discipline scientifiche quali l'informatica e la statistica, può essere qualificata come un'immagine scientifica e può essere affiancata ad altre immagini scientifiche del consumatore emerse nel corso della storia. Per capire più precisamente cosa sia un'immagine scientifica del consumatore e che cosa distingua l'immagine scientifica del consumatore proveniente dai *big data* dalle altre, serve innanzitutto soffermarsi brevemente sul concetto di consumatore. Con 'concetto di consumatore' si intende qui il significato minimo che il termine 'consumatore' assume nel linguaggio ordinario e in quello giuridico. Il consumatore, in base a tale significato, è una persona che partecipa a una o più delle fasi del ciclo del consumo (che possono essere considerate, quanto meno in linea generale, la fase della persuasione, quella dell'acquisto e quella della fruizione). Questa è la base comune a tutte le diverse immagini scientifiche del consumatore: esse si formano a partire dagli interventi realizzati da diverse discipline scientifiche sul concetto di consumatore al fine di renderlo più dettagliato[1]. Tale concetto, infatti, non precisa quale comportamento contraddistingue il consumatore, ma solo che un individuo è un consumatore se partecipa a una o più delle fasi del ciclo del consumo. Se vogliamo riprendere una distinzione filosofica tradizionale, possiamo allora dire che ogni immagine scientifica del consumatore consiste in una concezione del consumatore, ossia in una particolare declinazione del concetto di consumatore appena visto: ogni immagine scientifica, attraverso l'applicazione di idee proprie di determinate discipline scientifiche a tale concetto, aggiunge a quest'ultimo una serie di indicazioni relative al comportamento che contraddistingue il consumatore.

[1] La nozione di immagine scientifica appena delineata proviene dalla nozione di immagine scientifica dell'uomo proposta da Wilfrid Sellars. Per Sellars, un'immagine scientifica dell'uomo è «l'applicazione all'uomo di una cornice di concetti dotata di una certa autonomia. Dal punto di vista metodologico, infatti, ciascuna teoria scientifica è una struttura che viene costruita in un diverso "luogo", e sulla base di differenti procedure, all'interno del mondo intersoggettivamente accessibile delle cose percepibili» (W. Sellars, *La filosofia e l'immagine scientifica dell'uomo* (1962), trad. it. Roma, Armando Editore, 2007, p. 65).

Il consumatore nella prospettiva dei big data*: alcune considerazioni filosofico-giuridiche*

Il presente articolo esamina come la nozione di consumatore sia influenzata dall'uso dei *big data*. La risultante immagine del consumatore viene caratterizzata come una concezione del consumatore e confrontata con altre concezioni del consumatore. Dopo questo confronto, viene preso in considerazione il modo in cui questa concezione sembra emergere all'interno del GDPR.

The consumer in the perspective of big data: some legal-philosophical considerations

The paper examines the way in which the notion of consumer is influenced by the use of big data. The resulting image of the consumer is characterized as a conception of the consumer and is compared with other conceptions of the consumer. After this comparison, the way in which this conception seems to appear in the GDPR is taken into consideration.

Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019), pp. 133-160

La portabilità dei dati personali

Jessica Bozzoli*

Sommario: 1. La portabilità dei dati personali, introduzione. – 2. Inquadramento ed applicazione del diritto alla portabilità nel Regolamento UE 2016/679. – 3. Le diverse «forme» di portabilità. – 4. Conclusioni.

1. *La portabilità dei dati personali, introduzione*

L'evoluzione tecnologica ha trasformato l'economia e le relazioni sociali semplificando la circolazione dei dati all'interno dell'Unione europea ed il loro trasferimento verso i paesi terzi e tra le organizzazioni internazionali. Proprio per la notevole diffusione di tali dati si richiede un elevato livello di protezione così da garantirne la tutela come diritto fondamentale[1], come ribadito anche nel Considerando n. 1 del nuovo regolamento sulla protezione dei dati personali da bilanciare con altri diritti e libertà fondamentali riconosciuti dall'ordinamento europeo, anche in relazione all'evoluzione tecnologica. Come esplicitato nel Considerando n. 6, "tale evoluzione richiede un quadro giuridico più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È necessario che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per i privati che per gli operatori economici e le autorità pubbliche"[2].

* Master di II livello in Diritto Privato Europeo - Università La Sapienza (Roma).

[1] Cfr. G. Finocchiaro, "L'equilibrio titolare/user nel diritto d'autore dell'Unione europea", in «Diritto dell'informazione e dell'informatica», 3, maggio-giugno, 2016, p. 499. Si osserva inoltre che anche la Carta dei diritti fondamentali dell'Unione europea tutela la protezione dei dati personali all'art. 8, oltre a tutelare la vita privata all'art. 7. Per un commento alla Carta Cfr. R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini, *Carta dei diritti fondamentali dell'Unione europea*, Milano, Giuffrè, 2017; Cfr. S. Peers, T. Hervey, J. Kenner, A. Ward, *The EU charted of foundamental rights*, Oxford, Hart Pub Ltd., 2014.

[2] Considerando n. 6 del Regolamento UE 2016/679.

Tra i diritti riconosciuti all'interessato, nel nuovo regolamento si aggiunge il diritto alla portabilità, il quale, soddisfacendo l'obiettivo di facilitare la circolazione, la copia o la trasmissione dei dati da un ambiente informatico all'altro, ne soddisfa un secondo, cioè potenziare il controllo degli interessati e più in generale dei singoli individui sui dati personali che li riguardano e dai medesimi forniti. In questo modo il diritto alla portabilità assicura agli interessati un ruolo attivo nell'ecosistema dell'informazione[3].

Al diritto in parola viene inoltre riconosciuto un ruolo rilevante nell'incoraggiare la concorrenza tra i singoli servizi nel quadro della strategia per il mercato unico digitale facilitando il transito dei dati personali da un titolare all'altro nell'erogazione dei servizi[4].

Nonostante il diritto alla portabilità sia definito come un nuovo diritto[5], se ne osservano forme preesistenti, come la portabilità del numero di telefono (in particolare nella risoluzione contrattuale nei servizi di

[3] V. Linee guida del Gruppo di Lavoro Articolo 29 per la protezione dei dati 16/IT WP 242 rev.01, p. 4 reperibile al sito https://www.garanteprivacy.it/regolamentoue/portabilita. Il diritto alla portabilità, come indicato nelle linee guida, permette di «riequilibrare il rapporto tra interessi e titolari del trattamento tramite l'affermazione dei diritti e del controllo spettanti agli interessati in rapporto ai dati personali che li riguardano».

Per un approfondimento Cfr. C. Buzzacchi, "La politica europea per i big data e la logica del single market. Prospettive di maggiore concorrenza?" , in «Concorrenza e mercato», vol. 23, n. 1, gennaio 2016, p. 153; Cfr. G.M. Ruotolo, "La lotta alla frammentazione geografica del mercato unico digitale: tutela della concorrenza, uniformità, diritto internazionale privato", in «Diritto del commercio internazionale», 2, giugno 2018, p. 501; Cfr. G. Petruzzella, "Big data, competition and privacy: a look from the antitrust perspective", in «Concorrenza e mercato», vol. 23, n. 1, gennaio 2016, p. 15; Cfr. R.H. Weber, "Data portability and big data analytics. New competition policy challenges", in «Concorrenza e mercato»; vol. 23, n. 1, gennaio 2016, p. 59 ss.; S. Sica, V. D'Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, Cedam, 2016;

[4] Per fare un esempio, tale diritto consente alle banche di fornire ulteriori servizi attraverso l'impiego dei dati personali inizialmente raccolti per un diverso servizio, come la fornitura di servizi energetici. Chiaramente ciò avviene sempre sotto in controllo dell'utente. Il diritto alla portabilità favorisce così la creazione di nuovi servizi. Cfr. C. Buzzacchi, "La politica europea per i big data e la logica del single market: prospettive di maggiore concorrenza?", cit., p. 153;

[5] Cfr. A. Ricci, *I diritti dell'interessato*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da Finocchiaro, Bologna, il Mulino, 2017, pp. 219-220; Cfr. S. Familiari, "Il diritto alla portabilità dei dati: origine e prospettive per il futuro", in «Ciberspazio e Diritto», n. 3, dicembre 2016, pp. 403 ss.;

La portabilità dei dati personali

Il presente articolo, dopo aver preso in rassegna i diversi "diritti alla portabilità" previsti nel nostro ordinamento, esamina in particolare la disciplina giuridica del diritto alla portabilità dei dati personali, previsto all'art. 20 del Regolamento UE 2016/679 (GDPR), mettendo in risalto la sua ambivalenza, tra l'esigenza di protezione dei dati e quella di libera circolazione.

Personal Data Portability

This paper, after it reviewed the different "rights to portability" provided for by the Italian law, examines particularly the legal regulation of the right to data portability, under the in art. 20 of Regulation EU 2016/679 (GDPR), highlighting its ambivalence, between the need of data protection and the requirement of free flow.

Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019), pp. 161-176

Finalità di ricerca scientifica ed eccezioni alla disciplina della protezione dei dati personali*

Roberto Cippitani**

Sommario: 1. Dati personali e attività di ricerca. – 2. Finalità scientifiche. – 3. Finalità scientifiche ed eccezioni ai diritti della persona interessata. – 4. Utilizzi successivi e principio di granularità. – 5. Conservazione dei dati e conseguenze sui diritti dell'interessato. – 6. Equilibrio tra protezione dei dati personali e libertà di ricerca.

1. *Dati personali e attività di ricerca.*

La grande disponibilità di dati è oramai considerata uno dei principali strumenti di indagine da parte della comunità scientifica.

Ciò accade principalmente in ambito biomedico. La maggior parte delle attuali conoscenze in questo campo deriva dallo studio sistematico di campioni biologici umani conservati in biobanche, contenenti materiali come sangue, cellule, tessuti e DNA, nonché informazioni associate al campione e riguardanti il donatore[1].

Inoltre, l'uso di massicce quantità di dati è di cruciale importanza anche in altri ambiti scientifici[2], dalle scienze sociali, a quelle tecniche,

* L'articolo è uno dei risultati dell'attività nell'ambito del Progetto "Umbria Biobank: Start up per una Biobanca in Umbria", Progetto PRJ-1506, Azione 2.3.1, POR-FESR 2014-2020, cofinanziato dall'Unione Europea e dalla Regione Umbria.

** Professore straordinario di Diritto privato, Università degli Studi di Perugia, Dipartimento di Medicina. Membro del Centro di Ricerca «Rights and Science». Insegna Biodiritto e Diritto dell'informatica e informatica forense. Si occupa di aspetti giuridici ed etici della ricerca scientifica.

[1] Tra gli altri, v. J. Eder, H. Gottweis, K. Zatloukal, "IT Solutions for Privacy Protection in Biobanking", in «Public Health Genomics», vol. 15, 2012, pp. 254-262.

[2] Per un quadro generale, v. i documenti della Commissione Europea che si occupano di ricerca, come "Guidance How to complete your ethics self-assessment"; "Roles and Functions of Ethics Advisors/Ethics Advisory Boards in EC-funded Projects"; "Euro-

alle discipline che si occupano della natura e dell'ambiente[3].

Di particolare rilievo giuridico sono i problemi posti dall'utilizzo di dati personali e cioè «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"), così come definiti dall'art. 4 n. 1 del vigente Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito, utilizzando l'acronimo in inglese "GDPR")».

Molto spesso i dati personali raccolti durante le ricerche rilevano aspetti particolarmente delicati della persona e quindi rientrano nella definizione di "dati sensibili" (v. art. 9 GDPR), come appunto i dati sanitari e genetici[4], ma anche quelli che rivelino opinioni di carattere politico o le convinzioni sociali, nella ricerca delle scienze sociali[5].

pean Textbook on Ethics in Research" e il "Syllabus on Ethics in Research. Addendum to the European Textbook on Ethics in Research".

[3] Sui problemi etici e giuridici sollevati dalle collezioni di risorse biologiche vegetali e animali, si permetta il rinvio a R. Cippitani, "La investigación científica sobre los recursos genéticos: reflexiones jurídicas", in C. Mayorga Muñoz, F. Treggiari (a cura di) *Biodiversidad y Conocimimientos Tradicionales*, Ediciones Universidad de la Frontera: Santiago del Cile, pp. 125-147.

[4] In particolare, i dati genetici, in precedenza non direttamente considerati dalle fonti come dati personali (v. la "Convenzione di Strasburgo n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati personali" del 1981 del Consiglio d' Europa e la Direttiva 95/46/CE dell'Unione Europea del 24 ottobre 1995), ma comunque qualificati come tali dalla letteratura (cfr. M. D'amico, «Il trattamento pubblico dei dati sensibili: la disciplina italiana a confronto con il modello europeo, in Il diritto comunitario e degli scambi internazionali», Vol. n. 4, 2002, p. 817 ss.) e dai documenti emessi da organismi sovranazionali (V. l'"Explanatory Memorandum" della Raccomandazione n. R (97)5 del Comitato dei Ministri del Consiglio d'Europa (v. par. 41) il documento di lavoro sui dati genetici, adottato il 17 marzo 2004 dall'*Article 29 Data Protection Working Party*, par. III, p. 5), oggi vengono definiti dal GDPR come dati particolari (v. artt. 4, n.13 e 9, par. 2, GDPR) e corrispondono ai dati che, prima dell'entrata in vigore di tale testo normativo, venivano definiti come "sensibili".

[5] Vedi, tra i documenti che ricordano la necessità di adottare cautele nel trattamento dei dati personali sensibili nella ricerca in campo sociale, Commissione Europea, "Ethics in Social Science and Humanities", 2018, disponibile in Internet al seguente indirizzo (http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_ethics-soc-science-humanities_en.pdf); Id., "Guidance Note for Researchers and Evaluators of Social Sciences and Humanities Research", 2010, disponibile in Internet al seguente indirizzo: https://ec.europa.eu/research/participants/data/ref/fp7/89867/social-sciences-humanities_en.pdf; Social Research Association, "Ethical Guidelines", 2003, disponibile in Internet al seguente indirizzo: http://the-sra.org.uk/wp-content/uploads/ethics03.pdf.

Finalità di ricerca scientifica ed eccezioni alla disciplina della protezione dei dati personali

La grande disponibilità di dati è oramai considerata uno dei principali strumenti di indagine da parte della comunità scientifica.
Quando i dati si riferiscono a persone fisiche, essi sono oggetto della disciplina di cui al Regolamento UE 2016/679, che detta regole specifiche, molto più di quanto accadeva nella previgente Direttiva, nel caso in cui il trattamento avvenga per finalità scientifiche. Ciò allo scopo di promuovere la ricerca scientifica, considerata una libertà fondamentale dalla Carta dell'Unione Europea, e di realizzare la libera circolazione delle conoscenze, così come previsto dalle fonti comunitarie.
In particolare, per raggiungere tali obiettivi, il GDPR prevede delle eccezioni ai diritti riconosciuti alla persona interessata. Tali eccezioni sono comunque soggette al rispetto di un complesso di principi, come la proporzionalità, che mirano a trovare un equilibrio tra libertà di ricerca e diritto alla protezione dei dati personali.
Fondamentali per assicurare detto equilibrio risultano l'erborazione di codici di condotta e altri strumenti da parte dei titolari del trattamento che operano in ambito scientifico.

Finalità di ricerca scientifica ed eccezioni alla disciplina della protezione dei dati personali

Nowadays, the large availability of data is considered one of the main tools of survey by the scientific community.
When data relate to individuals, they are subject to the discipline of Regulation EU 2016/679, which lays down specific rules, much more than ones set up in the previous Directive, in the event that data are processed for scientific purposes. This is in order to promote scientific research, considered a fundamental freedom by the Charter of the European Union, and to achieve the free movement of knowledge, as provided for by Community sources.
In particular, to achieve these objectives, the GDPR provides for exceptions to the rights granted to the data subject. However, those exceptions are subject to the respect of a set of principles, such as proportionality, which aim at finding a balance between the freedom of research and the right to the protection of personal data.
The development of codes of conduct and other tools by the controllers carrying out research activities are fundamental to ensure this balance.

Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019), pp. 177-196

L'evoluzione del trattamento dei dati religiosi: dalla legge 675/1996 al Regolamento (UE) 2016/679

Giovanni Franco*

Sommario: 1. Introduzione. – 2. Il fattore religioso all'interno della Legge 675/1996. – 3. Il fattore religioso all'interno del Codice della Privacy. – 4. La protezione dei dati personali nella Chiesa cattolica. – 5. Il caso dello "sbattezzo": la ricomposizione del conflitto ad opera del Garante per la protezione dei dati personali e del Tribunale di Padova. – 6. Il sistema di protezione del dato religioso secondo il Regolamento Europeo 2016/679.

1. *Introduzione*

In questo magmatico periodo storico sospinto da due "forze" normative coesistenti, da un lato il Regolamento (UE) 2016/679 e dall'altro il d.lgs. 196 del 30 giugno 2003 (conosciuto anche come *Codice della Privacy*)[1], emerge una disciplina dei dati personali a carattere religioso che apre nuovi possibili scenari di trattamento, pur sempre nel solco della loro tradizionale tutela legislativa giacché appartenenti a quella categoria di dati che incidono sulla sfera più intima dell'individuo.

* Si è laureato in Giurisprudenza a pieni voti e ha frequentato il corso di perfezionamento in "Data Protection e Data Governance. Dal Codice Privacy al Regolamento Generale Europeo sulla Protezione dei Dati" presso l'Università degli Studi di Milano.

[1] In forza dell'espressa delega al Governo prevista dall'art. 13 della legge di delegazione europea 2016-2017 n. 163 del 25 ottobre 2017 (G.U. n.259 del 6-11-2017), è stato pubblicato in G.U. n° 205 del 4 settembre 2018 il Decreto Legislativo 10 agosto 2018, n. 101, intitolato *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);* tale decreto legislativo, entrato in vigore il 19 settembre 2018, ha apportato modifiche al Codice in materia di protezione dei dati personali, adeguando la normativa interna a quella europea.

L'importanza di siffatta *species* di dati personali è stata ben espressa dalle seguenti parole del Prof. Stefano Rodotà tratte dal suo discorso conclusivo tenutosi durante la Conferenza internazionale sulla protezione dei dati del 2004: «Senza una forte tutela dell'informazioni che le riguardano, le persone rischiano sempre di più d'essere discriminate per le loro opinioni, credenze religiose, condizioni di salute: la privacy si presenta così come un elemento fondamentale della società dell'uguaglianza. Senza una forte tutela dei dati riguardanti le convinzioni politiche o l'appartenenza a partiti, sindacati, associazioni, i cittadini rischiano d'essere esclusi dai processi democratici: così la privacy diventa una condizione essenziale per essere inclusi nella società dell'informazione»[2].

Oggetto del presente elaborato è l'analisi della disciplina del trattamento dei dati religiosi con lo scopo di mettere in luce la sua evoluzione all'interno dell'ordinamento nazionale italiano dalla legge 679/1996 sino alle novità apportate dal Regolamento (UE) 2016/679, con uno sguardo rivolto anche alla normativa confessionale per alcune riflessioni di natura comparatistica.

2. *Il fattore religioso all'interno della Legge 675/1996*

I dati di natura religiosa erano menzionati all'art. 22 della legge 675/96 e venivano considerati parte dell'ampia categoria dei dati sensibili; la disposizione aveva natura eccezionale rispetto al complesso di norme concernenti i dati c.d. comuni e comportava, per un verso, una forza derogatrice alla norma e, per l'altro, l'esigenza di una sua interpretazione restrittiva al fine di evitarne un'eccessiva espansione. Vi era quindi la scelta – confermata anche nella normativa successiva – che alcuni tipi di dati dovessero essere assoggettati a norme specifiche per la loro incisività nella sfera privata; il legislatore, all'interno della generale categoria dei dati personali, delimitava così un più ristretto nucleo di dati attinente alla sfera più intima dell'individuo.

[2] Trattasi della Conferenza internazionale sulla protezione dei dati del 14, 15 e 16 settembre 2004 a Cracovia, in Polonia. Il discorso integrale di Rodotà è disponibile su http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1049293.

L'evoluzione del trattamento dei dati religiosi: dalla legge 675/1996 al Regolamento (UE) 2016/679

L'elaborato ha ad oggetto l'analisi dell'iter evolutivo della disciplina nazionale sul trattamento dei dati religiosi dalla legge 675/1996 sino alle recenti novità apportate dal Regolamento (UE) 2016/679, con uno sguardo rivolto alla legislazione confessionale per alcuni spunti di riflessione di natura comparatistica.
I dati di natura religiosa sono stati da sempre sottoposti ad una peculiare tutela da parte della normativa in materia di protezione dei dati personali in ragione della loro appartenenza a quella categoria di dati che incidono profondamente sulla sua sfera più intima dell'individuo; questa impostazione è stata altresì confermata dal Regolamento (UE) 2016/679 che introduce perfino significativi elementi di novità tali da prospettare nuovi scenari di trattamento dei dati idonei a rilevare le convinzioni religiose.

L'evoluzione del trattamento dei dati religiosi: dalla legge 675/1996 al Regolamento (UE) 2016/679

The contribution concerns the analysis of the evolutionary process of the national discipline on the processing of religious data from law No 675/1996 up to the recent changes made by European Regulation (EU) 2016/679; the paper concerns also confessional legislation for some comparative evaluations.
Religious data have always been subjected to a specific safeguard by data protection law because they belong to the most intimate category of personal data; this approach was also confirmed by European Regulation (EU) 2016/679 which introduces even significant new elements relating to processing of religious data.

Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019), pp. 197-239

Regolamento Europeo 2016/679: alcune normazioni di riferimento per declinare sul campo il principio dell'accountability

Fausto Mazzoni*

Sommario: 1. Introduzione. – 2. La Direttiva 95/46/CE. – 3. Le novità del Regolamento 679/2016, semplificazioni e oneri in capo al titolare e al responsabile del trattamento. – 4. ISO 31000:2010 Risk Management. – 5. ISO 27001:2017. – 6. ISDP 10003:2015. – 7. Conclusioni.

1. *Introduzione*

Il Regolamento (UE) 2016/679[1] del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al "trattamento di dati personali"[2], nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE[3], è diventato pienamente esecutivo a partire dal 25 maggio 2018. Le novità introdotte dal Regolamento, altresì denominato GDPR (*General Data Protection Regulation*), modificano radicalmente l'approccio adottato in tema di protezione dei dati personali, introducendo nel sistema legislativo di settore principi nuovi prima estranei al nostro ordinamento: di fatto, con la pubblicazione del GDPR in Gazzetta Ufficiale Europea il 4 maggio 2016, è iniziata una nuova stagione per i diritti dei cittadini europei nei rapporti

* Si occupa di progettazione, consulenza organizzativa e tecnologica, privacy governance a supporto dei sistemi informativi aziendali principalmente nel settore sanitario.

[1] Cfr. Garante per la protezione dei dati personali, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6264597 (gennaio 2018).

Cfr. eur-lex.europa.eu, http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679 (gennaio 2018).

[2] Cfr. Regolamento Europeo 2016/679, si rimanda alle definizioni contenute nell'art. 4 del regolamento 2016/679.

[3] Cfr. eur-lex.europa.eu, http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=LEGISSUM:l14012 (gennaio 2018).

con i soggetti che trattano dati personali come le amministrazioni pubbliche, le aziende e le organizzazioni in generale.

La piena esecutività del Regolamento cade in un periodo storico in cui, come mai prima, il problema della protezione e la sicurezza dei dati, personali e non, digitali o analogici, appare lontanissimo dall'essere risolto da parte di soggetti pubblici o privati che costruiscono il proprio business o i loro servizi sulla gestione di quei dati. La tecnologia e le buone pratiche che dovrebbero essere adottate per implementare sistemi sicuri di gestione del dato sono disattese, oppure utilizzate in modo approssimativo, addirittura utilizzate in modo inconsapevolmente non lecito. Troppo spesso si ripone nella semplice presenza tecnologica l'aspettativa di una protezione che appare di fatto più formale che sostanziale, per citare Bruce Schneier «se pensate che una tecnologia possa risolvere i problemi di sicurezza di un'organizzazione, allora non avete capito i problemi di sicurezza e non avete capito la tecnologia»[4]. I numeri raccontano più delle parole questa drammatica situazione, per citare il Rapporto Clusit[5]: «il 2016 è stato complessivamente l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber" e dei relativi impatti, non solo dal punto di vista quantitativo ma anche e soprattutto da quello qualitativo. Rispetto al 2015, nel 2016 la crescita percentuale maggiore di attacchi gravi si osserva verso le categorie "Health" (+102%), "GDO/ Retail" (+70%) e "Banking / Finance" (+64%), seguite da "Critical Infrastructures" (+15%)». Anche l'autorità garante in materia di protezione dei dati personali ha confermato questo trend, quantificando in nove miliardi di euro i danni subiti dalle aziende italiane causati da incidenti di sicurezza, rilevando come meno del 20% di queste investa in modo adeguato per proteggere il proprio patrimonio informativo evidenziando altresì come il settore pubblico, dal punto di vista degli investimenti in sicurezza, non risulti essere più virtuoso[6]. Tornando alle considerazioni contenute nel rapporto Clusit relativo all'anno 2016, è importante riportare un ulteriore allarme: «Senza mezzi termini, il quadro che emer-

[4] Cfr. B. Schneier, "Schneier on Security" - https://www.schneier.com/books/secrets_and_lies/pref.html (gennaio 2018).

[5] Cfr. Rapporto Clusit 2017, https://clusit.it/rapporto-clusit/ (gennaio 2018).

[6] Cfr. Garante per la protezione dei dati personali, "Relazione annuale dell'autorità Garante per la protezione dei dati personali" - http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6458037 (gennaio 2018).

Regolamento Europeo 2016/679: alcune normazioni di riferimento per declinare sul campo il principio dell'accountability

L'elaborato analizza alcune best practice di riferimento che consentono ad un titolare del trattamento di implementare misure tecniche ed organizzative adeguate con la finalità di soddisfare i requisiti del Regolamento Europeo 2016/679 rispetto ai trattamenti di dati personali effettuati.

Regolamento Europeo 2016/679: alcune normazioni di riferimento per declinare sul campo il principio dell'accountability

This paper explores some best practices that help a data controller to implement appropriate technical and organisational measures for the purpose of demonstrating compliance with Regulation (EU) 2016/679 of processing operations by data controllers.

Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019), pp. 241-269

Il trattamento dei dati nel Sistema Sanitario Nazionale italiano alla luce del Provvedimento del Garante del 7 marzo 2019

Manlio d'Agostino Panebianco*

1. *Premessa*

L'analisi del trattamento dei dati, alla luce dell'entrata in vigore del Regolamento Generale sulla Protezione dei Dati (comunemente conosciuto anche come GDPR, *General Data Protection Regulation*) [1], nell'ambito sanitario italiano si presenta con una serie di peculiarità e particola-

* Professore a c. di "Criminalità Economica e Crimini Informatici" presso al Corso Triennale in Scienze della Mediazione Linguistica (Cl. Laurea L-12), SSML (Padova/Milano) - Membro del Comitato Tecnico del Centro Studi di Ricerche sull'Intelligence Economica e Security Management della Università degli Studi di Roma Tor Vergata (Roma) - Afferente e membro del comitato scientifico del "B-ASC" Centro di ricerca dell'Università degli Studi di Milano Bicocca - Membro del GdL sulla Privacy del Coordinamento Italiano dei Distretti del Rotary Club International.

[1] Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

rità, anche e proprio per l'assetto specifico conferito dal Legislatore a tale settore nel corso degli anni.

Alla luce del Provvedimento dell'Autorità Garante per la protezione dei dati personali[2] del 7 marzo 2019, recante "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario", è opportuno evidenziare gli aspetti salienti che regolamentano il rapporto di fiducia di tra il Servizio Sanitario Nazionale Italiano ed il paziente (l'interessato).

L'impresa sanitaria è una rete complessa con diversi attori: pazienti, personale medico, paramedico e amministrativo (Huerta et al., 2016); la sua complessità deriva proprio dal rapporto tra risorse, personale, strumenti, pazienti, organizzazione interna, protocolli e procedure da rispettare (Berwick e Leape, 1999)[3].

Oltretutto, questa rete si estende ben oltre quei confini apparentemente visibili, sebbene siano facilmente circoscrivibili. Infatti, in Italia l'ambito sanitario è costituito da una collaborazione di attori pubblici e privati, collocati a diverso livello e con diverse caratteristiche e funzioni: il Sistema Sanitario Italiano[4] è formato da un insieme di Aziende Unità Sanitarie Locali, Aziende Ospedaliere, Aziende Universitarie, Istituti di ricovero e cura a carattere scientifico, che operano nell'ambito delle attività di prevenzione, diagnosi, cura e riabilitazione erogate dal sistema sanitario, nonché di quelle amministrative correlate alle citate attività[5]. A questi, si aggiungono tutti gli attori privati che erogano (in proprio o per conto del SSN) le relative prestazioni e cure.

Quindi, proprio in ragione dei diversi ruoli e funzioni (alcune delle quali assumono la veste di vere e proprie esternalizzazioni, delegate attraverso il processo di convenzionamento, concessione, accreditamento, e/o appalto di un servizio pubblico), il trattamento dei dati deve essere letto alla luce, nonché integrato, con altre disposizioni legislative, anche di

[2] Registro dei provvedimenti n. 55.

[3] F. Baldassarre, F. Ricciardi, R. Campo, "Analisi di processo nel settore sanitario: colli di bottiglia e possibili miglioramenti", in «Economia e Commercio», serie V, anno XXV, n. 0, 2016.

[4] Il Decreto legislativo 30 dicembre 1992, n. 502, lo definisce come il «complesso delle funzioni e delle attività assistenziali dei Servizi sanitari regionali e delle altre funzioni e attività svolte dagli enti e istituzioni di rilievo nazionale».

[5] Cfr. R. Tommasi, *La difesa della privacy nella sanità*, Maggioli Editore, Santarcangelo di Romagna, 2007.

Il trattamento dei dati nel Sistema Sanitario Nazionale italiano alla luce del Provvedimento del Garante del 7 marzo 2019

Il trattamento dei dati nell'ambito sanitario italiano è tra i più peculiari: in primis, perché è un sistema completamente misto, vedendo la compartecipazione di attori pubblici e privati (ivi compresi alcuni che in assenza di limiti e cautele potrebbero utilizzare le informazioni in modo improprio); sia perché, proprio in ambito sanitario, si instaura il rapporto di fiducia più delicato (medico-paziente) in cui la riservatezza medica meglio si coniuga con quella della privacy. Lo stesso è altresì quello a maggior sensibilità (poiché caratterizzato da particolari categorie di dati relativi alla salute ed alle patologie) e rischio per l'elevato numero di soggetti che sono coinvolti nei trattamenti. Per tale ragione, dopo l'entrata in vigore del GDPR, sembra opportuno soffermarsi sugli effetti applicativi del Provvedimento del Garante per la Protezione dei Dati Personali del 07/03/2019, che indica univocamente le linee guida da adottare per garantire il diritto degli interessati.

Il trattamento dei dati nel Sistema Sanitario Nazionale italiano alla luce del Provvedimento del Garante del 7 marzo 2019

Data processing in the Italian healthcare sector is one of the most peculiar: firstly since it's a full mixed system, with the participation of public and private actors (including some, that in the absence of limits and cautions, could improperly use information and data); moreover, because in the health sector, is established the most delicate relationship of trust (doctor-patient) where *medical confidentiality* best combines with that one of privacy. Moreover making it the one with greater sensitivity, as characterized by of special categories of personal data relating to health and pathologies, and as well more risky, due to the large number of subjects involved in the treatments. For this reason, after the entry into force of the GDPR, it seems appropriate to focus on the effects of the Provision of the Italian Authority of Data Protection of 07/03/2019, which clearly gives guidelines to be adopted to guarantee a legal processing and the right of the data subject.

Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019), pp. 271-294

Insider Threat: Analisi dei recenti attacchi al protocollo di Internet BGP. La debolezza dei sistemi basati sulla fiducia

Andrea Razzini*

Sommario: 1. Introduzione. – 2. Descrizione del BGP. – 3. Messaggi scambiati tramite il protocollo BGP. – 4. Considerazioni sulla sicurezza di BGP. – 5. Tipologie di attacchi al BGP. – 6. Storia degli incidenti al protocollo BGP. – 6.1. Aprile 2010, "China Telecom". – 6.2. Novembre 2018: un nuovo caso "China Telecom". – 7. L'iniziativa MANRS. – 7.1. I Principi del MANRS e le Azioni. – 7.2. I partecipanti del progetto MANRS e le Linee guida per l'implementazione delle Azioni. – 7.3. La checklist delle informazioni. – 8. Miglioramenti alla sicurezza del BGP. – 9. Rimedi oggi disponibili in rete. – 10. Siti web che offrono servizi di Monitoring. – 10.1. BGPMon.net. – 10.2. RouteViews. – 10.3. RIPE RIS. – 11. Progetti e ricerche per il miglioramento della sicurezza BGP. – 11.1. OpenBMP. – 11.2. Il protocollo BGPSec. – 11.3. SCION - Scalability, Control and Isolation of Next Generation Networks. – 11.4. La Blockchain e il protocollo BGP. – 12. Punti aperti. – 13. Conclusioni.

1. *Introduzione*

Il BGP o Border Gateway Protocol, nato nel 1989, rappresenta uno dei meccanismi fondamentali preposti al funzionamento di tutta l'infrastruttura di Internet, spesso definito come il vero collante della rete. Da allora ad oggi sono stati emanati più di centottanta documenti sul BGP come risulta dall'elenco disponibile sul sito www.IETF.org e che riguardano vari aspetti del funzionamento di questo protocollo. Il BGP rimane tuttora un protocollo semplice, affidabile ma fondamentalmente insicuro.

* L'autore si è laureato in Ingegneria Elettronica al Politecnico di Milano e in Fisica all'Università degli Studi di Milano. Possiede una lunga esperienza maturata in multinazionali in ambito Telecomunicazioni di cui una decina di anni nel settore Sicurezza Informatica. Possiede diverse certificazioni come ad es. CISSP, CEH e CCSK e lavora attualmente come consulente in una multinazionale occupandosi frequentemente di attività sia di Threat Assessment / Risk Assessment che di Vulnerability Analyses e Penetration Testing. [le idee espresse rappresentano opinioni personali].

È il meccanismo che deve controllare l'instradamento del traffico dati in tutta la rete. La rete Internet può essere rappresentata come un grafico di nodi, a loro volta chiamati sistemi autonomi, che sono in pratica una collezione di routers controllati da un service provider, con collegamenti creati tra questi dispositivi per scambiarsi informazioni di instradamento e raggiungibilità. Lo scopo principale del BGP è quello di tenere aggiornati tutti i dispositivi per trasmettere e ricevere traffico dati senza errori. Ciò riguarda l'invio e la ricezione delle mail, la navigazione sui siti Web ed in generale la trasmissione di messaggi che rappresentano i cosiddetti pacchetti dati. Come altri protocolli di rete, nati senza requisiti di sicurezza espliciti, o come diremmo oggi senza la security by design, esso e' soggetto a varie tipologie di attacchi, spesso classificati come "perdite di instradamento" . Ma, come vedremo in seguito, una delle minacce in Internet più pericolose per la privacy e la sicurezza dei dati può derivare dall'interno, rendendo più difficile una protezione efficace. La situazione già abbastanza difficile dal punto di vista tecnico, si complica ulteriormente se aggiungiamo i dubbi circa un utilizzo legittimo da parte degli operatori di rete delle proprie apparecchiature e connessioni. La guerra commerciale tra USA e Cina che coinvolge ultimamente anche i fornitori cinesi di apparati di telecomunicazione non fa che rendere più fosco il quadro entro cui cercare soluzioni al problema. Varie accuse di manipolazione di schede madri destinate alle infrastrutture critiche americane, poi accuse ad un altro fornitore di frode commerciale e violazione di sanzioni internazionali, fanno emergere la tensione che si sta preparando tra le superpotenze, per primeggiare in campo tecnologico. Numerose sfide digitali si presentano all'orizzonte nei prossimi mesi: 5G, Blockchain, Intelligenza Artificiale, Quantum Computing, Criptovalute e Big Data saranno il terreno di grandi battaglie sia sulle capacità tecniche che sugli aspetti diplomatici e di potere. Cercare un coordinamento tra le grandi aziende del pianeta su aspetti di sicurezza può diventare estremamente difficoltoso.

2. *Descrizione del BGP*

Il BGP (Border Gateway Protocol) fu definito come standard dall'organismo internazionale IETF (Internet Engineering Task Force) e descritto originariamente nel documento RFC 1105. Oggi è giunto

Insider Threat: Analisi dei recenti attacchi al protocollo di Internet BGP. La debolezza dei sistemi basati sulla fiducia

Anche nel mondo digitale si assiste ad una erosione e svalutazione del concetto di fiducia. Quando Internet è nata, tutti i computer connessi in rete erano considerati "fidati". Il numero dei sistemi e degli utenti era allora molto ristretto, così essi non necessitavano di meccanismi per conoscere ogni identità che inviava dati in rete. Man mano che i sistemi e gli utenti crescevano, quella fiducia iniziale diminuiva e i primi meccanismi di sicurezza venivano aggiunti per supportare l'identificazione di chi contattava altri utenti in rete. Come vedremo in seguito, oggi più che mai, i sistemi che si fondano sulla fiducia, siano essi i protocolli di rete, le tecnologie sottostanti, le questioni legate alla privacy, tutti necessitano di essere resi più sicuri. Sarà dunque questo il filo conduttore del presente articolo in cui si intende presentare un'analisi dei recenti casi di dirottamento del traffico dati in Internet, dovuto ad attacchi ad uno dei protocolli più diffusi in rete.

Insider Threat: Analysis of recent attacks on the BGP Internet protocol

Even in the digital world there is an erosion and devaluation of the concept of trust. When the Internet was born, all the computers connected to the network were considered "trusted". The number of systems and users was then very restricted, so they did not need mechanisms to know each identity that sent data over the network. As systems and users grew, that initial trust diminished and the first security mechanisms were added to support the identification of those contacting other users on the network. As we will see later, today more than ever, systems based on trust, whether they are network protocols, underlying technologies, privacy issues, all need to be made more secure. This will therefore be the common thread of this article in which we intend to present an analysis of the recent cases of data traffic hijacking on the Internet, due to attacks on one of the most widespread protocols on the net.

Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019), pp. 297-310

Cybercrime e *criminal profiling*: i nuovi approcci delle tecniche investigative nell'era tecnologica

Andrea Scirpa*

Sommario: 1. Cybercrime: evoluzione tecnologica ed introduzione ai crimini informatici. – 2. *Criminal profiling*: *excursus* storico e metodi. – 3. *Criminal profiling* nell'era tecnologica. – 4. I primi approcci di *criminal profiling* applicati ai crimini contro la persona.

1. *Cybercrime: evoluzione tecnologica ed introduzione ai crimini informatici*

L'evoluzione tecnologica, con il crescente utilizzo di Internet e dei social network, ha inevitabilmente alterato i concetti di "vicinanza", "comunicazione" e di "anonimato"; ha ridotto i rapporti umani ed empatici, incrementando, conseguentemente, quelli virtuali.

Il Cyberspazio è un luogo tutt'ora sconosciuto e possiamo affermare di conoscere e di utilizzare solo una piccola parte di esso. È un ecosistema complesso: se utilizzato in maniera corretta e controllata, permette di produrre e scambiare informazioni a distanza ed è una grande risorsa, non solo per coloro che utilizzano Internet a fini lavorativi, ma altresì come mero mezzo di comunicazione e scambio di opinioni.

Attraverso la rete, gli utenti hanno la possibilità di entrare in contatto con persone che vivono dall'altra parte del globo senza dispendio di energie, in modo rapido e privo di costi; se utilizzato in maniera corretta e lecita, Internet è una fonte inesauribile di informazione.

Il Cyberspazio però, offre anche la possibilità di compiere qualsivoglia atto – non di rado, illegale – con la percezione di rimanere impuni-

* Laureata in Giurisprudenza presso l'Università degli Studi di Milano, ha conseguito un Master in Criminologia presso Cenaf. Collabora con la Cattedra di "Informatica Giuridica" dell'Università degli Studi di Milano come cultore della materia ed è componente del comitato di redazione della Rivista Scientifica «Ciberspazio e Diritto».

ti: lo schermo infatti, oltre a fungere da filtro tra il soggetto agente e la potenziale vittima di reato, permette al primo di agire indisturbato ovunque si trovi, senza il bisogno di essere fisicamente sulla scena del crimine[1].

Invero, una delle differenze sostanziali tra crimine tradizionalmente inteso e cybercrime è il fatto che i criminali informatici non necessitano di trovarsi fisicamente sulla scena del crimine. Attraverso un semplice programma, infatti, inserito all'interno della rete organizzativa ed azionato in qualsiasi momento, l'autore del reato potrà realizzare, indisturbato, il proprio disegno criminoso[2].

Come è noto, l'uomo è solito adattarsi ai cambiamenti. Negli ultimi trent'anni, con l'avvento di Internet, si sono notevolmente ridotti i rapporti umani e, di converso, sono incrementati quelli virtuali.

I soggetti caratterialmente più deboli hanno trovato nella rete un riparo sicuro entro cui agire: la percezione comune infatti, è quella di parlare e di interagire con un dispositivo informatico o telematico e non, invece, con una persona reale, con un volto, dei sentimenti e delle emozioni. Allo stesso modo, il crimine si è dovuto reinventare e adattare ai cambiamenti sociali, e ha trovato nella rete un nuovo territorio di caccia, all'interno del quale muoversi in autonomia.

Molteplici sono stati i tentativi svolti al fine di indicare una condotta illegale attuata mediante l'utilizzo di dispositivi informatici o telematici; tuttavia, il termine più utilizzato – e che è entrato a far parte del lessico comune – è quello di "cybercrime".

Per cybercrime si intende il "reato nel quale la condotta o l'oggetto materiale del crimine sono correlati a un sistema informatico o telematico (*computer as a tool*), ovvero perpetrato utilizzando un tale sistema o colpendolo (*computer as a target*)"[3].

Il cybercrime assume diverse forme all'interno del Cyberspazio.

Primo fra tutti, troviamo il cyberstalking, definito come la trasposizione digitale del reato di atti persecutori di cui all'art. 612-*bis* c.p.

[1] Cfr. N. Nykodym, R. Taylor, J. Vilela, "Criminal profiling and insider cyber crime", *Digital Investigation*, Elsevier, University of Toledo, OH, USA, (2005) 2, pp. 261-267.

[2] Cfr. N. Nykodym, R. Taylor, J. Vilela, "Criminal profiling and insider cyber crime", Digital Investigation, Elsevier, University of Toledo, OH, USA, (2005) 2, pp. 261-267.

[3] Cfr. Treccani, *cybercrime*, lessico del XXI secolo.

Cybercrime e criminal profiling: i nuovi approcci delle tecniche investigative nell'era tecnologica

Questo articolo intende mettere in luce come il crimine, nella sua accezione tradizionale, sia cambiato con l'era tecnologica. Si è cercato di svolgere una panoramica delle nuove figure di reato introdotte con la Legge 23 dicembre 1993 n. 547 e con la Legge 18 marzo 2008 n. 48, al fine di evidenziare come il crimine si sia adeguato alle nuove tecnologie e, dunque, ai mutamenti sociali.
Come è noto però, con l'evoluzione tecnologica non è cambiato solo il crimine in senso stretto: i mezzi di contrasto, le tecniche investigative, si sono dovute adeguare e si sta cercando di introdurre delle nuove tecniche di *profiling* in grado di prevenire e prevedere il verificarsi del *cybercrime*.
Il *criminal profilng* infatti, non è una scienza, ma una tecnica investigativa; in collaborazione con le altre discipline, però, può senza alcun dubbio contribuire in maniera rilevante al contrasto del crimine.

Cybercrime e criminal profiling: i nuovi approcci delle tecniche investigative nell'era tecnologica

This article aims to highlight how crime, in its traditional sense, has changed in the technological age. An overview of the new forms of crime introduced by Law 23 December 1993 n. 547 and Law 18 March 2008 n. 48 has been attempted in order to highlight how crime has adapted to new technologies and, therefore, to social changes. As is known, however, with the technological evolution, not only crime in the strict sense has changed: the means of contrast, as well as the investigative techniques, have had to adapt and new profiling techniques able to prevent and predict the occurrence of cybercrime are being introduced.
In fact, criminal profiling is not a science, but an investigative technique: in collaboration with other disciplines, however, it can, without any doubt, contribute in a relevant way to the fight against crime.

Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019), pp. 311-328

Cyberstalking, le condotte tipiche e i soggetti coinvolti

Samanta Stanco

sommario: 1. Introduzione. – 2. Le condotte tipiche. – 3. Il persecutore. – 4. La vittima. – 5. Un confronto tra stalking e cyberstalking.

1. *Introduzione*

Lo stalking è reato ormai disciplinato in molti Paesi del mondo. In particolare, la tradizione più autorevole è quella nordamericana: negli Stati Uniti l'attenzione legislativa per il fenomeno ha iniziato a svilupparsi negli anni Novanta nell'ambito del cosiddetto "star-stalking", ossia lo stalking rivolto a celebrità e a personaggi di spicco nel mondo dello spettacolo.

Il verbo inglese "to stalk" raggruppa un'ampia gamma di significati e, letteralmente, è traducibile come "avvicinarsi di soppiatto": indica quindi il comportamento del predatore, che in questo caso perseguita la propria vittima con pedinamenti, appostamenti, telefonate assillanti, comparendo nei luoghi da lei frequentati, ossessionandola con la propria presenza e procurandole stati di ansia e di insicurezza. Indipendentemente dalle singole giurisdizioni, pertanto, lo stalking è inteso come il volontario, malvagio e ripetuto seguire e molestare una persona, tale da mettere in pericolo la sua incolumità. Non si tratta di un crimine costituito da un singolo atto ma, al contrario, può essere realizzato con una moltitudine di comportamenti differenti, spesso difficili da identificare e distinguere dalle condotte lecite: molti di essi, infatti, se considerati individualmente, sono legittimi e consentiti, ed è solo presi collettivamente,

* Laureata in Giurisprudenza presso l'Università degli Studi di Milano, ha conseguito il perfezionamento in "Criminalità informatica e investigazioni digitali – cyberbullismo, cyberstalking, reati d'odio tra adulti e adolescenti e tutela dei soggetti deboli". Collabora con la Cattedra di "Informatica Giuridica" dell'Università degli Studi di Milano come cultore della materia ed è componente del comitato di redazione della Rivista Scientifica «Ciberspazio e Diritto».

nel contesto, che diventano assillanti o minacciosi e quindi tali da integrare il reato in esame.

Una novità importante in questo campo è stata apportata dalla tecnologia: Internet si è infatti rivelato terreno fertile per lo stalking, in quanto offre grandi possibilità di comunicazione e interazione, anche con persone sconosciute, e dà all'utente una – molto spesso illusoria – garanzia di anonimato. Avendo caratteristiche del tutto peculiari, lo stalking telematico è stato ribattezzato "cyberstalking" e qualificato come l'uso di Internet, della e-mail o di altri mezzi di comunicazione elettronica al fine di molestare una persona. Negli ultimi anni si sta assistendo a un netto prevalere delle ipotesi telematiche rispetto a quelle dello stalking tradizionale e vi sono tutti i presupposti per ritenere che questa situazione sia destinata ad accentuarsi ulteriormente.

2. *Le condotte tipiche*

Pur trattandosi di un quadro piuttosto fumoso, per abbracciare tutte le ipotesi di questo *crime* possono essere ravvisati quattro comportamenti tipici dello stalker:

i) un'attività di sorveglianza nei confronti della vittima, di gran lunga facilitata dall'invasività delle nuove tecnologie, spesso usate dall'utente come funzioni ludiche (basti pensare ai recenti servizi di geolocalizzazione), ma in realtà efficaci strumenti di controllo per i molestatori;

ii) un'attività di comunicazione (sovente ossessiva) nei confronti della vittima;

iii) un'attività di ricerca di contatto, che si colloca a metà tra un pedinamento elettronico e un "aggiramento" compiuto collegandosi ad amicizie, anziché contattando direttamente la vittima;

iv) un'attività di controllo, spesso all'insaputa della vittima.

Queste quattro categorie beneficiano di due aspetti fondamentali: la possibile incompetenza tecnologica del soggetto controllato, che può condurlo a fornire informazioni preziose allo stalker (si pensi, a titolo esemplificativo, ad una configurazione di una privacy policy di Facebook debole), e la possibilità di correlazione dei dati offerta dalla tecnologia.

Cyberstalking, le condotte tipiche e i soggetti coinvolti

Lo stalking ha oggi assunto caratteristiche peculiari a seguito dell'avvento delle nuove tecnologie, che l'hanno reso un fenomeno ancora più insidioso e invasivo, ribattezzato "cyberstalking", termine con cui si identifica l'uso di dispositivi di comunicazione elettronica al fine di molestare un'altra persona. Il presente saggio ne analizza alcuni aspetti fondamentali, quali le condotte tipiche, le figure del persecutore e della vittima e le differenze rispetto allo stalking tradizionale.

Cyberstalking, le condotte tipiche e i soggetti coinvolti

The advent of new technologies has led to the new phenomenon of cyberstalking, that is more insidious than traditional stalking due to its invasiveness. This paper examines what constitutes cyberstalking and harassment and discusses the way in which the Internet may facilitate such behavior, studying the role of the stalker and of the victim.

Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019), pp. 329-365

Procedimenti giudiziari, media e ruolo dei social: interazioni, problematiche e riflessioni

Guglielma Vaccaro*

Sommario: 1. Introduzione. – 2. Sviluppi, limiti ed evoluzione della figura del giornalista. I cosiddetti programmi "infotainement". – 3. Diritto di cronaca, privacy e minori. Il caso di James Bulger. – 4. Dall'aula giudiziaria al set televisivo: Un giorno in Pretura. – 5. Dal 2000 ad oggi: prevalenza dei social su programmi televisivi e processi? – 6. Chi l'ha visto: battaglie per la verità, colpi di scena in diretta e sospetti di accanimenti. – 7. Il caso Scazzi: rilevanza mediatica e ruolo dei social sul procedimento giudiziario. – 8. Il caso di Roberta Ragusa. – 9. Il caso di Elena Ceste: una tragedia divenuta farsa? – 10. Il caso Gambirasio e il processo Bossetti: tracimazione sui social, nuove frontiere e derive. – 11. Il caso Macchi. – 12. Il caso Vannini, proteste in piazze virtuali e reali. – 13. Il caso Pitzalis e il caso Mastropietro: utilizzo dei social come rivalsa? Il confronto con il caso di Jessica Faoro. – 14. I social possono incrinare la definitività delle condanne? Ancora il caso Scazzi. – 15. La "strage di Erba": quando a difendersi sono le vittime. – 16. Conclusioni.

1. *Introduzione*

L'epoca attuale si potrebbe definire l'età d'oro della comunicazione, e questo grazie alle tecnologie informatiche, che consentono di acquisire informazioni in quantità inimmaginabile sino a pochi anni fa e, soprattutto, in tempo reale; per contro, è fatto notorio che il mondo del-

* Avvocato, da anni si interessa di questioni legate al ruolo dei social nella cronaca e di alcune vicende prese in esame nel presente studio ha avuto esperienza diretta; le opinioni espresse nel presente documento, in mancanza di diverso riferimento, sono di responsabilità esclusiva dell'autrice e non necessariamente riflettono la posizione ufficiale dei soggetti coinvolti a vario titolo nei casi oggetto della presente analisi; le parti delle sentenze analizzate, in mancanza di diverso reperimento opportunamente indicato, hanno fonte giornalistica. Queste riflessioni sono dedicate alle vittime nascoste dal brusio della troppa comunicazione.

la comunicazione *latu sensu* professionale stia attraversando una profonda crisi strutturale che coinvolge il settore della carta stampata e del giornalismo "classico". A questo proposito, chi scrive pone come data simbolica di inizio del mutamento (o della rivoluzione) il 2001[1], anno della diretta in mondovisione del primo attacco terroristico su larga scala del XXI secolo. In estrema sintesi, con l'avvento di nuove tecnologie di interazione (ovvero implementazione e diffusione capillare di Internet, dispositivi portatili e prezzi accessibili delle connessioni), comunicazione e notizie vanno sempre più veloci, mentre l'informazione su carta o le redazioni piene di telefoni che squillano faticano a tenere il ritmo, fiaccate dalla concorrenza di strumenti meno costosi se non a costo zero. Da tempo l'*iter* di una notizia oramai è il seguente: lancio con un post sul sito o, più spesso, sulla pagina Facebook di riferimento – i dettagli verranno successivamente narrati con aggiornamenti successivi o in un articolo dedicato –; nel frattempo il primo annuncio online ha raccolto centinaia se non migliaia di chiose, cesellature, pareri favorevoli e contrari… e una dose fisiologica di insulti, oramai immancabile per ogni categoria di avvenimenti, dai più tragici ai più leggeri.

Accanto a pochi altri argomenti particolarmente sentiti, la cronaca nera si mostra ancora oggi[2] l'argomento che cattura l'interesse del (spesso distratto) utente finale e ingenera con ragionevole probabilità l'auspicato ritorno economico per editori alle prese, per i motivi già indicati, con perdite di tirature e copie di anno in anno; pertanto attualmente è possibile osservare una crescente interazione tra fatto di cronaca e media che se ne occupano, con pressoché immediata esternazione di opinioni che si moltiplicano come in un caleidoscopio attraverso commenti su pagine dedicate nei social[3], i quali, a loro volta, determinano scambi e concessioni tra

[1] Il giorno 11 settembre 2001 Alle 8.46 del mattino un aereo, un Boeing 767, il volo American Airlines 11 si schiantò sulla torre nord del World Trade Center, a Manhattan, nel centro di New York; mentre si cercava ancora di capire cosa fosse successo, diciassette minuti dopo un altro Boeing 767, il volo United Airlines 175, si schiantò contro la Torre Sud a favore di decine di telecamere, dirette straordinarie e collegamenti online, allora una novità.

[2] I "grandi casi" di cronaca che hanno appassionato l'Italia, ovviamente, non sono una prerogativa dell'epoca attuale, nuova è l'interazione attraverso le nuove strumentazioni tecnologiche; sono ancora vive nella memoria collettiva vicende risalenti a mezzo secolo fa ed oltre e debitamente documentate da reportage di giornalisti e scrittori e foto in bianco e nero che ritraggono aule giudiziarie stracolme di gente attenta e curiosa.

[3] D'ora in poi, nel presente articolo, con il termine "social" o "social network"

Procedimenti giudiziari, media e ruolo dei social: interazioni, problematiche e riflessioni

Accanto a pochi altri argomenti, la cronaca nera si mostra ancora oggi un ottimo collettore di interessi e discussioni; di conseguenza, è possibile osservare una crescente interazione tra fatto di cronaca e media che se ne occupano con immediata diffusione di opinioni che si moltiplicano e alimentano attraverso commenti sulle piattaforme social con pagine espressamente dedicate; quando la vicenda approda in un'aula giudiziaria, tali nuove interazioni comunicative possono influire sul dibattimento? Il presente studio si pone come obiettivo di fornire se non risposte almeno qualche riflessione al riguardo.

Judicial procedures, average and role of the social: interactions, problem list and reflections

Similar to few other issues, the crime appears a good collector of media discussions today; it is possible to observe an increasing interaction among true story and an immediate diffusion of opinions that multiplies comments with, also, pages dedicated to this "debate"; when crime comes to trial, can such communicative interactions influence the judicial debate? The present study aims to provide some reflection in this direction.