Ciberspazio e diritto, vol. 18, n. 57 (1-2017), pp. 3-29

La *net neutrality* alla luce del Regolamento UE n. 2120/2015 e delle Linee Guida BEREC

Costanza Martani

Sommario: 1. Definizione della *net neutrality*. – 2. Diritto di accesso a Internet. – 3. Ragionevolezza del *traffic management*. – 4. Trasparenza del *network management*. – 5. Conclusioni.

1. *Definizione della* net neutrality

La neutralità della rete ha rappresentato, e rappresenta tuttora, uno dei maggiori fattori di espansione di Internet. Nonostante tale principio sia un punto cardine dell'ecosistema digitale, non risulta di così evidente ovvietà né l'individuazione dei suoi elementi identificativi, né tantomeno il delinearsi di cosa debba comportare, in concreto, una corretta applicazione di suddetto principio.

La net neutrality viene definita tradizionalmente come principio di progettazione il cui vero significato «starebbe nell'idea che una rete informativa pubblica massimamente utile aspiri a trattare tutti i contenuti, siti e piattaforme allo stesso modo. Ciò permette alla rete di trasportare ogni forma di informazione e di supportare ogni tipo di applicazione»[1], tale per cui «due o più utenti che usufruiscono di un servizio fornito da *providers* diversi ma di uguale qualità devono poter scambiare dati godendo di questa pari qualità di servizio senza discriminazioni poste sulla base di un *hardware* particolare, *software*, rete sottostante, lingua, cultura, handicap o tipologie di dati»[2], rappresentando pertanto il principio di neutralità della rete un principio di regolamentazione volto a limitare discri-

[1] Tim WU esplicita tale definizione nel suo sito web http://www.timwu.org/network_neutrality.html.

[2] Cfr. F. Dell'Isola, "La neutralità della rete nella regolamentazione internazionale comunitaria e nazionale: una questione risolta?", in «Rivista della Cooperazione Giuridica Internazionale», vol. 35, maggio - agosto 2010, p. 1.

minazioni dannose o anticompetitive da parte di operatori di reti e fornitori di servizi[3].

Il concetto di net neutrality così com'è andato delineandosi negli ultimi anni, però, non può da un lato dirsi ridotto a un principio di non discriminazione e di parità di trattamento dei dati circolanti in rete né, dall'altro, si può aderire ad una interpretazione così rigida ed assolutizzante di tale principio, la quale potrebbe risultare contraria agli interessi degli utenti finali e trasformarsi essa stessa in un ostacolo allo sviluppo di Internet.

Risulta pertanto necessario, per una migliore comprensione della portata del concetto di net neutrality e dei pericoli connessi a una possibile elusione di tale principio, individuare preliminarmente sia i soggetti che si muovono nella rete, che gli ulteriori principi che la ispirano, i meccanismi di funzionamento della stessa e le conseguenti problematiche che la interessano. Gli attori che svolgono un ruolo centrale nell'ambito dell'online sono essenzialmente due: gli *Internet Service Provider* (ISP) i quali forniscono i servizi di accesso a Internet (IAS) propedeutici al consumo di contenuti online, e i *Content and Application Provider* (CAP) ossia i fornitori di servizi, contenuti e applicazioni. Tra questi ultimi sono ricompresi sia gli editori tradizionali (televisivi, cinematografici e della carta stampata che utilizzano anche lo strumento della rete), sia gli *user generated contents*, ossia gli utenti che caricano in rete i propri contenuti altresì chiamati *prosumer* (al tempo stesso consumatori e fornitori di contenuti), sia infine i c.d. OTT (*Over the Top*), ossia quelle grandi Internet Company quali Google, Yahoo, Facebook, Skype, etc., le quali, essendo prive di una propria infrastruttura, agiscono per l'appunto "al di sopra della rete". Gli OTT nello scenario attuale si pongono in concorrenza con le tradizionali aziende di telecomunicazioni (c.d. Telco) agendo, da un lato in modo complementare attraverso per esempio il social networking, e dall'altro sostituendosi alle Telco come nei casi dei servizi di messaggistica (si pensi a Whatsapp), posta elettronica e telefonia vocale.

Nel complesso, dunque, è possibile riscontrare sempre maggior varietà di applicazioni e servizi online, da quelli tradizionali (motori di ricerca, e-mail, blog, etc.), ai servizi multimediali (video/foto sharing,

[3] Cfr. Studio della Commissione per il mercato interno e la protezione dei consumatori, "*Network Neutrality: challenges and responses in the EU and in the US*" - IP/A/IMCO/ST/2011-02, maggio 2011.

La net neutrality alla luce del Regolamento UE n. 2120/2015 e delle Linee Guida BEREC

La neutralità della rete, intesa come eguaglianza dei dati trasmessi in rete, rappresenta un principio fondamentale di Internet che ne ha permesso la crescita, garantendo inoltre la libertà di comunicazione e manifestazione del pensiero e quindi la libertà della rete. Il crescente sviluppo di Internet ha però reso necessario operare un trattamento dei dati trasmessi in rete. L'interpretazione del principio di neutralità della rete non deve pertanto essere rigido e assoluto ma utile e necessario e, allo stesso tempo, deve impedire un abuso dei sistemi correttivi di controllo del traffico dati. Il Regolamento UE n. 2120/2015 e le Linee Guida BEREC si sono pertanto posti l'obiettivo di fornire norme comuni a livello comunitario per far sì che Internet continui a essere una piattaforma aperta, individuando in tal guisa i tre pilastri della neutralità della rete: il diritto di accesso ad Internet, la ragionevolezza del *traffic management*; la trasparenza del *network management.*

Net neutrality in the light of EU Regulation No 2120/2015 and BEREC's Guidelines

Net neutrality, understood as network data equality, is a fundamental principle that has allowed for growth of the Internet and to safeguard net freedom. However, the development of the Internet requires network management. In fact, net neutrality interpretation should not be strict or absolute, but useful and necessary and, at the same time, it has to prevent abuses of traffic management. The EU Regulation No 2120/2015 and the BEREC's Guidelines have set the goal to provide for common rules at Community level to ensure the Internet remains a free and open platform by identifying the trhree pillars of net neutrality: the right to Internet access, the reasonable traffic management; the trasparency of network management.

Ciberspazio e diritto, vol. 18, n. 57 (1-2017), pp. 31-68

I *big data* come *common goods*[*]

Federico Ponte

1. *Introduzione: cenni minimi in ordine all'era dell'accesso (ai dati) e conseguente approccio metodologico*

Appaiono ormai del tutto scontate considerazioni sulla natura della nostra società che, se per certi versi è stata semplicisticamente rubricata come «post-industriale», per altri viene oggi positivamente qualificata come «società dell'accesso» e che di conseguenza, suggestivamente, invita a parlare di «era dell'accesso»[1].

Il merito del passaggio a questa nuova era è dovuto prevalentemente al procedimento di digitalizzazione dell'informazione, intendendosi con ciò la possibilità di fruire in un contesto tecnologico, attraverso l'ausilio degli elaboratori, di una quantità di dati in passato inimmaginabile: intere biblioteche potevano essere contenute prima in una stanza, ed oggi – quando ancora si ha sotto mano un supporto fisico – possono trovarsi in uno spazio capace di perdersi su una scrivania. Questa è la rivoluzione informatica.

[*] Il presente contributo è idealmente dedicato al collega Giulio Regeni, dottorando dell'University of Cambridge interessato alle tematiche dei beni comuni e prematuramente scomparso.

[1] L'entrata nel linguaggio comune di questa felice formulazione si deve in particolare a J. Rifkin, *The Age Of Access: The New Culture of Hypercapitalism, Where All of Life Is a Paid-For Experience,* New York, TarcherPerigee, 2000 trad. it. *L'era dell'accesso. La rivoluzione della new economy,* Milano, Mondadori, 2001. Dev'essere rilevato che l'accesso e più in genere il fenomeno delle nuove tecnologie è in costante mutamento e non può non essere compreso se non tenendo ben presenti le tecnologie che caratterizzano il periodo di riferimento, periodo spesso assai breve proprio in ragione della rapida evoluzione tecnologica.

Accanto alla rivoluzione informatica si è avuta una seconda rivoluzione, quella portata dalla rete Internet[2] e più in genere dall'evoluzione delle tecnologie di tipo comunicativo. Queste hanno esteso al di là di quanto era prima immaginabile la possibilità di fruire a distanza delle informazioni digitalizzate e sparse per il globo, prescindendo dall'effettiva collocazione fisica dei «contenitori elettronici» dei dati stessi. Si avverte quindi sempre meno, per tornare alla metafora dell'era dell'accesso, il bisogno di possedere una risorsa dal momento in cui questa è stata digitalizzata e messa in rete, divenendo pertanto fruibile ovunque e in ogni momento tramite *device* elettronici.

Ma la rivoluzione tecnologica, che ricomprende tanto quella informatica che quella comunicativa, non ha ancora avuto arresto. Dar conto dell'inarrestabile evoluzione esula dal presente contributo, ma per i fini che qui rilevano giova menzionare i fenomeni che caratterizzano la società tecnologica e più da vicino ci interessano, ossia il potenziamento delle infrastrutture comunicative, che ha reso più veloce il trasferimento di grandi quantità di dati[3], l'accentramento costante di questi dati in mano a pochi «colossi dell'informazione», siano essi la pubblica amministrazione o soggetti del settore privato, nonché le dinamiche *cloud*, che permettono ai titolari di *big data* di dislocarli su server remoti, potendo così conservare e analizzare i dati a costi nettamente inferiori a quelli che altrimenti dovrebbero sostenere *in loco*.

Così premesso l'attuale quadro tecnologico e venendo al tema che più propriamente s'intende trattare in questa sede, la scelta dei *big data* (in un'ottica che non mancherà di guardare il fenomeno confinante degli *open data* del settore pubblico) non è arbitraria: l'interesse si è infatti voluto focalizzare su un possibile bene comune piuttosto atipico anche prendendo ad esame le ricostruzioni della teorizzazione più orientate verso le nuove tecnologie, i cui contorni sono ancora poco nitidi.

[2] Per una ricostruzione dell'evoluzione dell'informatica e della rete Internet, attenta anche alle molteplici questioni giuridiche sottese, si veda P. Costanzo, "Contributo ad una storia della libertà d'informazione: le origini di Internet (1969-1999)", AA.VV., «Studi in onore di Aldo Loiodice», Bari, Cacucci 2012, pp. 691-710.

[3] Si pensi a tal riguardo all'attenzione, data anche dall'Unione Europea, alla promozione della diffusione della banda larga, inclusa tra gli obiettivi prioritari dell'agenda digitale europea. Cfr. Commissione europea, COM(2010)245, *Comunicazione della Commissione «Un'agenda digitale europea»*, del 19 maggio 2010, in part. par. 2.4.

I big data *come* common goods

Il presente contributo ha inteso calare nel contesto digitale, e più nello specifico nella dimensione venutasi a creare con l'emergere del fenomeno dei *big data*, una fattispecie che appartiene alla cultura giuridica occidentale dai tempi del diritto romano e che è arrivata sommessamente fino a noi, quale quella dei beni comuni.
I *big data* rappresentano uno dei più innovativi approdi tecnologici di cui il diritto è stato recentemente chiamato ad occuparsi, tanto in grado di potenziare la fruizione di determinati diritti fondamentali quanto di metterne altri a repentaglio.
La prospettiva costituzionalistica, considerata imprescindibile nelle attuali rivisitazioni della categoria di bene comune, mette chiaramente in luce quali sono gli aspetti su cui la nozione si fonda: finalizzazione alla tutela dei diritti fondamentali e della dignità umana, nonché attenzione posta sulla concreta possibilità di fruire del bene.
È risultato pertanto interessante mettere in connessione il portato tecnologico "big data" con la categoria giuridica dei beni comuni, in quanto ciò ha dato modo di vedere concretamente i limiti ed i punti di forza della stessa teoria calata in un contesto per cui non era stata pensata.

The 'big data' as 'common goods'

The present work aims to put in the digital context – and in a more specific way, in the dimension of the big data's emerging problem – the category of the common goods, which has belonged to the western legal theory since the roman law and quietly arrived up to the present day.
Big data represents one of the most innovative amongst technological issues which recently the law has been called to deal with, and they are able to enhance the fruition of some fundamental rights, as long as put in danger other ones.
The constitutional perspective – considered essential in the current revisions of the common goods category – clearly highlights which are the aspects founding its concept: first, finalization to the protection of the fundamental rights and human dignity, secondly the attention to genuine possibility in the fruition of the goods.
It was therefore relevant to connect the technological concept of the big data with the legal category of the common goods, in order to see the limitation and strengths of this theory in action, never considered for a context like this one.

Ciberspazio e diritto, vol. 18, n. 57 (1-2017), pp. 69-81

Morte degli utenti e persistenza dei dati: le soluzioni adottate dalle principali piattaforme tecnologiche

Giovanni Ziccardi

Sommario: 1. Facebook e la gestione dei defunti. – 2. Google, gli account inattivi e la rimozione degli utenti. – 3. La policy di Twitter. – 4. LinkedIn, Snapchat, Tumblr e le modalità di segnalazione. – 5. L'approccio di Instagram. – Riferimenti.

1. *Facebook e la gestione dei defunti*

La presenza in rete, e sui social network, di sempre più persone decedute è un fatto cui ci si dovrà ben presto abituare, a meno che gli ingegneri e i programmatori delle piattaforme non progettino gradualmente sistemi completamente diversi di gestione dei profili e di validazione delle identità e del ciclo di vita delle persone online. Questo è il motivo per cui occorre molta cautela nel sostenere che, ben presto, i profili degli utenti morti supereranno quelli dei vivi. Ciò avverrà soltanto se le piattaforme di social network non svilupperanno, *in itinere*, strumenti per gestire questa situazione. Si pensi, ad esempio, a un filtro che renda meno visibili, confini in determinate aree o, addirittura, elimini dall'ambiente social i profili di utenti defunti. Già Instagram, si vedrà, ha iniziato ad adottare alcuni espedienti per rendere *meno evidente* la presenza di utenti morti nell'ambiente di condivisione delle fotografie e nel relativo sistema di commenti e di collegamenti.

A oggi Facebook è il "luogo" più colpito da questo fenomeno, per diversi motivi.

Innanzitutto, i più giovani lo stanno abbandonando per migrare verso altri social network che vedono più coetanei presenti e, soprattutto, una minor presenza dei genitori (ad esempio Snapchat e Instagram), aumentando sensibilmente l'età media degli utenti su Facebook. D'altro canto, vi sono molti anziani che si stanno avvicinando alla piattaforma,

e sono in costante aumento grazie ai numerosi corsi che vorrebbero insegnare a usare Facebook agli esponenti della terza età. Infine, la piattaforma stessa, per com'è concepita e strutturata da un punto di vista tecnico, ha creato un ecosistema che tende a preservare il ricordo e la presenza delle persone, più che a eliminarlo.

Si sta, così, diffondendo in molti la convinzione che, a breve, saranno più i profili dei morti rispetto a quelli dei vivi, e la minaccia portata dalle tecnologie sarebbe, in questo caso, che Facebook si possa trasformare in un grande cimitero virtuale. Perdendo, ovviamente, gran parte del suo appeal.

Oltre a servire a mantenere egregiamente i contatti con i vivi o a gestire le ultime volontà tramite messaggi o proclami, è in occasione di una morte improvvisa e non annunciata che appare evidente a tutti la potenza del social network. Vi sono bacheche che continuano a mandare messaggi agli amici come se nulla fosse successo e profili che, nel caso nessuno abbia le password per gestirli, continuano a vivere imperterriti e a ricevere commenti e richieste di amicizia.

Non appena si diffonde la notizia della morte, gli spazi dei social network diventano suggestivi luoghi di cordoglio collettivo virtuale, dove si pubblicano fotografie, canzoni, video che presumibilmente sarebbero piaciuti al defunto, dove persone che vogliono continuare a scrivere s'incontrano sulla bacheca in una specie di veglia funebre digitale e avviano un nuovo dialogo reso possibile dalla tecnologia.

Si tratta, nella maggior parte dei casi, di un modo per mantenere vivo il ricordo, spesso non morboso, incivile e maleducato ma affettuoso, sociale e garbato, che ha reso il lutto anche digitale.

La funzione denominata *Memorial* di Facebook è certamente la più celebre e conosciuta implementazione della gestione della fine della vita degli utenti in un ambiente digitale.

Si tratta di un'opzione che permette di trasformare le pagine di un utente in un *account commemorativo,* ossia in uno spazio dove solo le conoscenze più strette possono intervenire con post o commenti.

In pratica, la pagina dell'utente defunto viene "cristallizzata" e ne è limitata la possibile interazione verso l'esterno.

Per attivare un profilo commemorativo occorre inviare agli addetti di Facebook una *death proof*, ossia una prova scritta della morte dell'utente – ad esempio un certificato di morte, o la fotografia di un necrologio,

Morte degli utenti e persistenza dei dati: le soluzioni adottate dalle principali piattaforme tecnologiche

In questo Articolo si analizzano le condizioni stabilite dalle policy dei principali social network e servizi informatici con riferimento alla morte di un utente o alla cessazione di utilizzo di un servizio da parte di un utente. Dalla possibilità di attivare profili commemorativi in Facebook all'azione di nominare un erede, sino alla gestione dei profili inattivi, si traccerà un panorama su come le tecnologie, oggi, gestiscano la morte degli utenti.

Death of users and data persistence: the solutions adopted by the main platforms

In this Article we analyze the conditions set by the policies of the major social networks and information services in relation to the death of a user or the cessation of use of a service by a user. The ability to activate commemorative profiles in Facebook, the action to appoint an heir and the inactive profiles management will trace a panorama of how technologies, today, can manage the user's death.

Ciberspazio e diritto, vol. 18, n. 57 (1-2017), pp. 85-111

Le ragioni dell'oblio

Simone Bonavita

Sommario: 1. Le conseguenze della rivoluzione digitale: persistenza, analisi, percezione e amplificazione della diffusione dei dati. – 1.1. La rivoluzione digitale. – 1.2. Persistenza. – 1.3. Analisi. – 1.4. Percezione e amplificazione. – 2. L'economia della reputazione. – 2.1. La misurazione della reputazione. – 3. La memoria digitale, la memoria umana e la memoria di Internet. – 3.1. La memoria umana. – 3.2. La memoria degli elaboratori. – 3.3. La memoria di Internet. – 4. Quale oblio?

1. *Le conseguenze della rivoluzione digitale: persistenza, analisi, percezione e amplificazione della diffusione dei dati*

Sta vivendo un momento storico di particolare interesse il diritto all'oblio, oggetto negli ultimi anni di numerose e discusse pronunzie giurisprudenziali.

Un diritto la cui definizione è spesso ricondotta alla sentenza della Corte Europea Consteja e che affronterà una nuova fase della propria vita a breve, quando il nuovo regolamento europeo sulla *data protection* entrerà in vigore.

Ma quali sono i motivi per i quali questo diritto si sta affermando solo negli ultimi anni e quali possibili futuri sviluppi questo potrà avere?

Rispondere a tali domande appare prodromico a ogni valutazione in merito allo stesso, nonché necessario a comprenderne i possibili futuri sviluppi.

1.1. *La rivoluzione digitale*

Appare necessario così soffermarsi brevemente sul fenomeno della cosiddetta "rivoluzione digitale" e sui cambiamenti che questa ha portato per quanto concerne, specificatamente, la disciplina del trattamento dei dati[1].

[1] Dubbia appare essere, a oggi, la definizione stessa di "dato". Di particolare interesse, e molto lucida, è la definizione di Pica, secondo cui il concetto di dato «esprime una registrazione elemen-

Due sono stati, probabilmente, i fenomeni che hanno condizionato quella che alcuni studiosi hanno definito "la quinta rivoluzione industriale"[2]: la diffusione di Internet e l'aumento della capacità di archiviazione e di elaborazione garantita dai calcolatori.

Così come la tecnologia ha consentito all'uomo il passaggio dall'età post-industriale all'età dell'informazione[3] così Internet ha determinato il mutamento di una realtà che si alimenta grazie alla presenza in rete dell'uomo[4] e che vive di differenti modelli economici rispetto al passato[5].

Non è dato sapere, per ora, se Internet, con i suoi paradigmi di comunicazione, abbia liberato le nostre menti e la nostra conoscenza o se sia diventata solo un mezzo di controllo per chi ha il potere di disporne, chiunque egli sia[6].

Così si contrappongono le posizioni di chi vede la rete come un fattore di emancipazione del singolo e delle libertà[7] a quelle di chi la considera come un possibile strumento per il controllo delle informazioni da parte di regimi autoritari[8]; altri autori, viceversa, sottolineano sia le opportunità che i rischi della diffusione di tali tecnologie, richiamando la necessità di porre sempre l'attenzione a che queste non siano utilizzate per limitare i diritti umani, ma piuttosto per renderne effettivo il loro rispetto[9].

tare nella memoria di un computer, pur non avendo una sua dimensione numerica prestabilita, che possa farlo ritenere una precisa unità di misurazione: nel linguaggio comune il termine dati ha invece una accezione più amplia, significando spesso l'insieme dei contenuti registrati nella memoria di un computer». Cfr. G. Pica, *Diritto penale delle nuove tecnologie*, Torino, UTET 1999. Tale definizione è stata recepita in dottrina, *inter alia*, da P. Perri, *Protezione dei dati e nuove tecnologie aspetti nazionali, europei e statunitensi*, Milano, Giuffrè 2007.

[2] Tale definizione è riconducibile a M. La Rosa, L. Regalia, E. Zucchetti, *Società e new economy*, Milano, Franco Angeli 2005.

[3] Cfr. D. Bell, "The coming of the post-industrial society", «The Educational Forum», volume 40, 1976, pp. 574-579.

[4] Per le complesse riflessioni sul punto, e per un utile riferimento bibliografico, si vedano F. Di Ciommo, *Evoluzione tecnologica e regole di responsabilità civile*, Napoli, ESI 2003, e E. Russo, *Evoluzione tecnologica e categorie civilistiche*, *Interpretazione della legge civile e ragione giuridica*, Padova, CEDAM 2003.

[5] Cfr. R. Wang, "Disrupting Digital Business: Create an Authentic Experience in the Peer-to-Peer Economy", «Harvard Business Review Press», Boston, 2015.

[6] Cfr. J. Goldsmith, J. Wu, *Who controls the Internet?: illusions of a borderless world*, Oxford, Oxford University Press 2006.

[7] Cfr. N. Negroponte, M. Asher, *Being digital*, New York, Vintage Book 1996.

[8] Cfr. E. Morozov, *The net delusion: The dark side of Internet freedom*, New York, Public Affairs 2012.

[9] Cfr. G. Sartor, "Human Rights and Information Technologies", «The Oxford Handbook of the Law and Regulation of Technology», in corso di pubblicazione. A p. 38 dell'articolo, l'autore sostiene che «in primo luogo i governi non dovrebbero privare gli individui dell'opportunità di eser-

Le ragioni dell'oblio

L'articolo esamina i motivi per i quali il diritto all'oblio sta vivendo un momento storico di particolare interesse, cercando di illustrarne gli interessi sottesi. L'autore si sofferma ad analizzare, in primo luogo, i cambiamenti che Internet ha determinato sulla persistenza, sull'analisi, sulla percezione e sulla amplificazione della diffusione dei dati, determinando un aumento del loro valore. L'autore s'interroga, infine, sulla configurabilità di tale diritto all'interno della società della comunicazione alla luce dell'imminente nascita delle tecnologie esponenziali.

The the right to be forgotten

The article explains the reasons according to which, the right to be forgotten is experiencing an extremely interesting moment, trying to point out the related interests. The author analyses, at first, the changes that Internet has brought on the persistence, analysis, perception and amplification of the data diffusion, leading to an increase in their value. Secondly, he asks himself about the configurability of this law within a communication society experiencing the birth of exponential technologies.

Ciberspazio e diritto, vol. 18, n. 57 (1-2017), pp. 113-169

Nuove tecniche d'investigazione nell'era digitale: il "malware" di Stato

Ferdinando Ditaranto[*], Roberta Ruggieri[**], Valentina Cupelli[***]

1. *Introduzione: la "rivoluzione" tecnologica e il processo penale*

Il progresso dell'*Information Technology* ha diffuso un modello di sviluppo sociale inedito e dalle potenzialità pressoché illimitate, determinando, nel concreto, la genesi di una mole abnorme di dati digitali che pervade sia l'ambito professionale sia quello ludico-domestico.

Sotto il profilo penale, ciò si traduce in un rapporto di stretta proporzionalità tra le potenzialità offerte da *Internet* e dal mondo virtuale e le metodologie investigative adottate dagli organi inquirenti. Le manifestazioni che si realizzano in rete hanno assunto nuove e rilevanti configurazioni caratterizzate, sotto certi profili, da un preoccupante impatto socia-

[*] Referente Area Reati Informatici presso la Sezione di Polizia Giudiziaria della Procura della Repubblica di Monza, Perfezionato in Computer Forensics e Investigazioni Digitali presso l'Università degli Studi di Milano, Informatico Forense, certificato CIFI (Certified Information Forensics Investigator) e ACE (Accessdata Certified Examiner). Le opinioni espresse non impegnano l'Istituzione di appartenenza. (Autore Paragrafi 2 e 6).

[**] Dottoressa in Giurisprudenza, Perfezionata in Data Protection e Investigazioni Digitali presso l'Università degli Studi di Milano, esperienza come stagista del comparto Network Development Mercato Italia presso multinazionale del settore *automotive*. (Autore Paragrafi 3 e 7).

[***] Dottoressa in Giurisprudenza, Perfezionata in Data Protection e Investigazioni Digitali presso l'Università degli Studi di Milano. Praticante presso studio legale di Milano specializzato in diritto penale dell'economia. (Autore Paragrafi 1,4 e 5).

le: gli operatori di polizia giudiziaria, infatti, ricorrono a nuovi approcci investigativi nel contrasto del *crimine ad alta tecnologia*[1], tenuto conto della capillare diffusione dei dispositivi digitali e delle piattaforme di *social network*.

Dagli anni Novanta, l'evoluzione degli strumenti comunicativi in correlazione all'avanzata delle nuove tecnologie portò il legislatore italiano alla rivisitazione del catalogo degli illeciti annoverati nel codice penale, sancendo il debutto dei *computer crimes* e, di conseguenza, della *digital evidence*, ovvero la fonte di prova digitale. Tale risorsa, investigativa prima e processuale poi, si connota per la sua immaterialità e fragilità, elevando alla massima potenza il rischio di alterazione e, nella peggiore delle ipotesi, di dispersione.

Prima della sottoscrizione della Convenzione di Budapest sul *Cybercrime* nel 2001 e la conseguente trasposizione nell'ordinamento italiano con la Legge 18 marzo 2008, n. 48, lo scenario investigativo e processuale nell'ambito dei *computer crimes* era contraddistinto dall'assenza di modalità operative standardizzate che spesso determinavano prassi e indirizzi giurisprudenziali equivoci ed oscillanti.

La ratifica della Convenzione sul *Cyber-crime* rappresenta una "pietra miliare" nell'evoluzione degli strumenti di contrasto alla criminalità ad alta tecnologia che ha consentito di fornire un'adeguata risposta alla proliferazione del fenomeno delinquenziale e, soprattutto, agli errori in fase investigativa. La normativa in esame ha ampliato il perimetro giuridico dei cosiddetti *reati informatici,* ha introdotti nuovi strumenti investigativi e ha definito, con accuratezza, i principi operativi da osservare nella trattazione delle evidenze digitali.

Mediante quest'ultima innovazione debutta sullo scenario italiano la disciplina della *Digital Forensics*, il cui obiettivo è quello di identificare, acquisire, conservare, interpretare e documentare in sede processuale le evidenze digitali, preservandone la genuinità mediante l'utilizzo di software specifici (*forensics tool*) ed osservando scrupolosamente i dettami annoverati nell'apparato delle linee guida di riferimento denominate *best practices*[2].

[1] M. Mattiucci, *I crimini ad Alta Tecnologia e l'Arma dei Carabinieri*, in www.marcomattiucci.it.

[2] M. Tonellotto, "Evidenza informatica, computer forensics e best practises", in «Riv. crim. vitt. sic.», n. 2/2014, secondo il quale «Per best practices si intende quell'insieme di comporta-

Investigazioni digitali 2.0 – il "malware di Stato"

L'autorità giudiziaria, per contrastare efficacemente le manifestazioni criminose che si realizzano nel sistema informatico e/o telematico, ricorre a strumenti tecnologici di nuova emersione, che sono soprattutto oggetto di ampio interesse da parte della giurisprudenza di legittimità.
Lo scopo del presente elaborato è da un lato fornire una panoramica sull'utilizzo di tali strumenti investigativi, quali l'*online surveillance* e l'*online search* o *one-time copy*, dall'altro lato, unendo le competenze tecniche, giuridiche e investigative, proporre una possibile regolamentazione normativa all'interno del codice di procedura penale.

The Digital Investigations – The "Trojan Horse"

To oppose effectively crimes in computer system and/or telematics system, the judicial authority uses new technological instruments which are the object of interesting examination by the Supreme Court.
The aim of this article is on the one hand to provide an overview of those investigative tools, namely online surveillance and online search or one-time copy, and on the other hand, combining the technical, investigative and legal expertise, to propose a possible regulation of those instruments inside the criminal procedure.

Ciberspazio e diritto, vol. 18, n. 57 (1-2017), pp. 171-203

Open Source Intelligence e *Deep Web*: scenari moderni delle Investigazioni Digitali

Antonio Sagliocca*

Sommario: 1. Introduzione. – 2. Le attività d'intelligence. – 3. L'*Open Source Intelligence*. – 4. La storia. – 5. Le fonti. – 6. I soggetti. – 7. Le tecniche e gli strumenti informatici. – 7.1. Motori di ricerca. Google e Search Engine Colossus. – 7.2. Wayback machine. – 7.3. Foca. – 7.4. Analisi delle fotografie: i dati Exif. – 7.5. Paterva Maltego. – 7.6. Shodan. – 7.7. Intelligence dei siti web. – 7.8. Social Media. – 7.9. Le banche dati pubbliche online. – 7.10. OSINT per la propria sicurezza. – 8. Il ciclo dell'*Open Source Intelligence*. – 9. Deep Web. – 9.1. Navigare nel web profondo. – 9.2. Deep Web e OSINT.

1. *Introduzione*

In un mondo sempre più digitalizzato, con la diffusione di Internet e l'abbattimento dei confini geografici, la possibilità di raccogliere online informazioni su avvenimenti, persone fisiche e società, si è fatta sempre più significativa. Quello che una volta era cartaceo ora, attraverso la digitalizzazione, potrebbe trovarsi sotto forma di informazione contenuta in un calcolatore e molte, sempre di più, sono le informazioni che nascono direttamente nel calcolatore elettronico andando a costituire fonti, tra le più diversificate. Tale vastità di contenuti, che spaziano ormai in tutti i settori principali della società, dai dati anagrafici, a quelli di salute, di sport e degli hobby, permette di passare da una mera e semplice ricer-

* Appassionato di nuove tecnologie, si occupa da vari anni di Investigazioni Private e Digitali, Open Source Intelligence ed Ethical Hacking. Studente di Sicurezza Informatica e Socio e Docente Clusit, ha alle spalle un'esperienza di oltre quindici anni in ambito IT Sistemistico e Tecnico. Agli inizi del 2000 ha partecipato al progetto di "alfabetizzazione informatica" organizzato dalla Municipalità a favore dei cittadini che si avvicinavano al mondo del Computer. Dall'A.A. 2015/2016 collabora con le Cattedre di Informatica Giuridica e Informatica Giuridica Avanzata dell'Università degli Studi di Milano.

ca online, come ad esempio digitando una parola in un motore di ricerca, a una vera e propria attività di intelligence con la possibilità quindi di raccogliere, analizzare e organizzare i contenuti. Quelle che sono attività d'intelligence nate prevalentemente in ambienti militari e dei servizi segreti, ora, grazie alla capillarità di Internet ed alla tecnologia, si trovano invece alla portata di tutti, provocando a certi livelli e, a seconda di chi se ne occupa, anche un rischio per la privacy e la sicurezza degli individui.

In quest'ottica già nel 2015 nella relazione sull'attività svolta durante l'anno, il Garante della *Privacy*, Antonello Soro, affermava: «la posta in gioco è alta e coinvolge la nostra riservatezza e con essa la nostra autostima: si pone un problema di libertà se in un'economia fondata sui dati non siamo capaci di proteggerli»

L'argomento è vasto e duplice, perché se da un lato la possibilità di disporre online di informazioni che riguardano persone fisiche e aziende assolve a compiti di informazione pubblica e trasparenza, indicando al contempo modernità dei tempi, dall'altro a causa della facilità con cui senza pensarci a sufficienza e con poca consapevolezza dei rischi gli utenti diffondono sui social network, blog e siti vari informazioni che li riguardano, sarà possibile per un soggetto terzo che abbia le competenze tecniche necessarie, reperire notizie che una volta aggregate, costituiranno un vero e proprio loro profilo.

Infine, recentemente, i soggetti dell'intelligence (pubblici e privati) hanno compreso che oltre al web classico che tutti conoscono, vi è un web più profondo, più grande di circa 500 volte quello normalmente conosciuto, il "*Deep* o *Dark Web*", all'interno del quale può essere molto proficuo orientare la propria attività di ricerca.

2. *Le attività d'intelligence*

«Il compito più difficile che ci compete in *intelligence* è quello di vedere il mondo così com'è, e non come noi vorremmo che fosse», disse nel 1991 il Direttore della CIA Robert Gates[1].

L'intelligence può essere definita come l'insieme di tutte le attività di raccolta, valutazione e analisi delle informazioni al fine di produrre "il sapere" necessario per il raggiungimento di determinati obiettivi o per saper prendere una decisione importante. "Sapere", che tanto più sarà

[1] Cfr. A. Teti, *Open Source Intelligence & Cyberspace,* Cosenza, Rubettino 2015, p. 31.

Open Source Intelligence *e* Deep Web*: scenari moderni delle Investigazioni Digitali*

Tra le attività investigative nel ciberspazio sta assumendo sempre più un ruolo da protagonista l'OSINT, ovvero l'Open Source Intelligence, l'Intelligence basata sulle "fonti aperte" cioè sulle fonti pubbliche e liberamente accessibili. Nell'Articolo, l'autore ne analizzerà le caratteristiche, gli strumenti e le tecnologie, partendo dalle origini, quando questa disciplina era riservata ai soli ambienti militari e dei servizi segreti, fino ad arrivare ai giorni nostri quando grazie alla diffusione di Internet e all'informatizzazione è divenuta strumento anche per le indagini di tipo giornalistico, per le investigazioni private, per attività di polizia, di marketing e per chiunque abbia le dovute conoscenze informatiche e doti investigative. E si spingerà nel Deep Web, il web sommerso, 500 volte più grande di quello comunemente conosciuto, nel quale si è capito ormai, che si potranno trovare informazioni "più appetibili" ai fini investigativi di quante se ne possano trovare "in superficie".

Open Source Intelligence and Deep Web: modern scenarios of Digital Investigations

Among the investigative activities in the cyberspace, the OSINT (Open Source Intelligence), based on "open sources", public sources and freely accessible, is assuming the role of protagonist. In the Article, the author will analyse its characteristics, tools and technologies, starting from the beginning, when this discipline was reserved only for the military and secret services, up to the present day when, thanks to Internet diffusion, they became powerful tools for the investigative journalism, the private investigation, police or marketing activities, and for anyone with the necessary computer and investigative skills. Moreover, he will lead you in the submerged web, the so called Deep Web, five hundred times bigger than the known one, in which one can find more stimulating information than those you could find "on the surface".

Ciberspazio e diritto, vol. 18, n. 57 (1-2017), pp. 207-240

Sperimentazione di una rete neurale per la predizione, attraverso l'intelligenza artificiale, del pericolo di stalking

Simone Icardi*

Sommario: 1. Introduzione al reato di stalking. – 2. Le principali classificazioni. – 3. 3. Ulteriori classificazioni. – 4. L'impatto sociale dello stalking. – 5. Stalking: patologia della comunicazione. – 6. Intelligenza artificiale: perché? – 7. Le reti neurali. – 8. Metodologia e strumenti della sperimentazione. – 9. Risultati. – 10. Conclusioni.

1. *Introduzione al reato di stalking*

Lo stalking è un fenomeno complesso che, negli ultimi anni, è apparso sempre più frequentemente nei fatti di cronaca nera riportati dai quotidiani e sui social network.

Il primo passo per comprendere questo tipo di condotta è analizzare le principali classificazioni, redatte dagli enti investigativi per l'analisi comportamentale, dello stalker, il suo rapporto con la vittima e i livelli di aggressività. Negli ultimi anni questo fenomeno è stato riconosciuto come reato, e in Italia è stata approvata la Legge 38/09[1] che prevede una condanna, per chi si macchia di tale reato, con pena fissata dai sei mesi ai quattro anni di reclusione. L'articolo 612-*bis* del codice penale regola i provvedimenti cautelari. Il reato deve essere reiterato e deve presentare una serie di condotte assillanti e atti persecutori che generano nella vittima un grave stato di ansia e paura fondata per la propria incolumità o per l'incolumità di una o più persone vicine a essa tale da costringerla a modificare le proprie abitudini quotidiane e la propria vita.

* Dottore in Scienze per l'investigazione e la sicurezza, dottore Magistrale in Scienze cognitive e processi decisionali. Cultore della Materia alla cattedra di Informatica Giuridica dell'Università degli Studi di Milano nell'area di ricerca sull'utilizzo delle nuove tecnologie intelligenti nell'investigazione.

[1] Conversione in legge, con modificazioni, del decreto-legge 23 febbraio 2009, n. 11, recante misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori (GU Serie Generale n. 95 del 24 aprile 2009). Entrata in vigore del provvedimento: 25 aprile 2009.

2. *Le principali classificazioni*

I principali studiosi australiani e americani[2] dell'ultimo decennio in ambito di comportamento persecutorio hanno stilati cinque profili con i quali è possibile classificare lo stalker: i) il risentito, ii) il bisognoso d'affetto, iii) il corteggiatore incompetente, iv) il respinto e v) il predatore.

L'utilità di questi cinque profili comportamentali è quella di sviluppare una certa capacità predittiva di tali dinamiche per permettere agli operatori del settore, forze dell'ordine e criminologi, di intervenire, consigliare e decidere in maniera maggiormente efficacie come affrontare i casi di stalking denunciati.

Il bisognoso di affetto

Questa tipologia di stalker è spinta dalla ricerca di una relazione sentimentale che può riguardare sia l'amicizia sia l'amore.

L'individuo sfrutta le dinamiche sviluppate in situazioni strettamente professionali, come la relazione tra paziente e psicoterapeuta.

Il persecutore cerca una vittima che, per caratteristiche superficialmente osservate, risponda al suo modello di partner: pensa, infatti, che la persona designata abbia bisogno di aiuto e quindi, tramite le proprie attenzioni, riuscirà a risolverne i problemi e a farla innamorare di lui.

La particolarità del rapporto instaurato spinge il persecutore a distorcere l'empatia mostrata o la richiesta di aiuto da parte dell'individuo che entra in relazione con lui.

Questa distorsione cognitiva comporta un'interpretazione della realtà diversa da quella che, effettivamente, si sviluppa tra i due individui e che dà inizio ai corteggiamenti. I corteggiamenti possono essere di due tipi: velati, o diretti, con un conseguente rifiuto da parte della persona che li riceve.

Il rifiuto è inizialmente negato e, successivamente, reinterpretato dal persecutore che sviluppa una convinzione: la vittima ha la necessità di superare il momento difficile e questa è la spiegazione della sua indisponibilità emotiva; secondo lo stalker, quindi, recuperata la lucidità inziale,

[2] Cfr. P.E. Mullen, M. Pathé, R. Purcell, *Stalkers and their victims*, Cambridge, Cambridge University Press 2009.

Sperimentazione di una rete neurale per la predizione, attraverso l'intelligenza artificiale, del pericolo di stalking

La prima parte del paper analizza gli studi inerenti a un fenomeno cresciuto negli ultimi anni: lo stalking. Lo stalking racchiude tutti quei comportamenti devianti costituiti da atti persecutori reiterati compiuti da un individuo nei confronti della sua vittima. Nella seconda parte del lavoro, il focus si sposta una ricerca svolta personalmente dall'Autore che aveva come obiettivo la programmazione di un prototipo di A.N.N. (Rete Neurale Artificiale) capace di imparare ad analizzare il comportamento dello stalker, definito da un database sperimentale, e predirne la pericolosità. La A.N.N. lavora su un database costruito con i parametri comportamentali scoperti dallo psicologo australiano Mullen, il quale ha delineato i *markers* comportamentali e la loro pericolosità basata sulla reiterazione. Il paradigma scientifico ha permesso all'Autore di costruire una rete funzionante; questo genere di architettura potrebbe essere uno spunto per lo sviluppo di future tecnologie applicabili nell'analisi comportamentale predittiva.

Experimentation of a neural network for the prediction, through artificial intelligence, of stalking danger

The first part of the paper analyzes the studies about one of the rising phenomenon of the last years: the stalking. Stalking concerns deviant behavior featured by repeated persecutor acts made by an individual toward his victim. In the second part of this work, the focus is on an experimental research the Author pursued, whose the achieve was to program an A.N.N. (Artificial Neural Network) prototype able to learn the stalker's behavior, typified from an experimental database, and to predict the stalker's dangerousness. The A.N.N. works on a database built with the behavioral parameters found by Australian psychologist Mullen, who has delineated the behavioral markers, and their dangerousness reiteration. This scientific paradigm let the experimental A.N.N. work; this architecture could be a fist hint for future technologies to be applied in predictive behavioral analysis.