Ciberspazio e diritto, vol. 16, n. 52 (1-2015), pp. 11-28

L'identità digitale: dalle nuove frontiere del Sistema Pubblico di Identificazione (SPID) alle problematiche legate al web

Valentina Amenta[1], Adriana Lazzaroni[2], Laura Abba[3]

"Prima che ci partiamo dal ragionamento del veder l'immagine pendent nell'aria, insegnaremo come si possa fare che veggiamo le imagini pendent nell'aria di qualsivoglia cosa; il che cosa mirabile più di tutte le meravigliose, principalmente, senza specchio, e senza l'oggetto visibile […] Ma diciamolo… come si veda un'imagine nell'aria in mezzo una camera, che non si veda lo specchio, nè l'oggetto della cosa visibile, e caminando intorno intorno vedrai l'imagine da tutte le parti."

Giovan Battista Della Porta, 1589.

1. Premesse sistematiche

Le riflessioni che seguiranno diventano una chiave di lettura importante in riferimento alla centralità dell'individuo nell'epoca delle reti e alle sue tutele. Se è vero che Internet si pone come il più grande strumento d'inclusione sociale, è anche vero che solleva inevitabilmente dei profili

[1] Dottore di ricerca in Diritto pubblico e dell'economia e Assegnista di ricerca presso l'Istituto di Informatica e telematica del Consiglio nazionale delle ricerche (IIT-CNR) per le tematiche della *Internet Governance*.

[2] Responsabile Scientifica dell'Istituto di Informatica e telematica del Consiglio nazionale delle ricerche (IIT-CNR) ed esperta di *Internet Governance*.

[3] Dirigente tecnologo dell'Istituto di Informatica e telematica del Consiglio nazionale delle ricerche (IIT-CNR) ed esperta di *Internet Governance*.

problematici in merito alla natura stessa dell'individuo. Si discute molto sulla commistione tra l'universo reale e quello virtuale, si cercano risposte a interrogativi complessi. Un "viaggio nel virtuale" porta alla formulazione di domande non solo centrate sulla rete in sé e per sé, ma soprattutto sull'idea di persona, oggi continuamente soggetta a mutamenti sociali, in cui gli spazi del virtuale non sembrano, come spesso invece si vuole affermare, una semplice sovrapposizione con il mondo reale, ma spazi intermedi nei quali è possibile costruire forme di relazionalità.

L'utilizzo della rete e delle varie applicazioni è in grado di determinare un ampliamento e una errata percezione dei confini del *Sé*. Presi nel vortice dei rapporti sociali, dividiamo disperatamente la nostra limitata attenzione, concedendo frammenti della nostra coscienza a ogni cosa o persona che richieda il nostro tempo. Nel farlo, rischiamo di perdere pian piano nella rete la nostra identità.

Internet è stata celebrata come il luogo utopico di uno spazio sociale dove età, genere ed etnia risulterebbero infinitamente riscrivibili, consentendo al soggetto di sperimentare forme post-moderne d'identità fluida e multipla. Nel *social web*, dove i processi sociali si articolano proprio sulla rete, gli utenti hanno la possibilità di esprimersi e di esporsi.

Se l'uso della rete era legato, tempo fa, alla consultazione dei siti web per acquisire informazioni, ora l'approccio comune sta radicalmente mutando: Internet non si presenta più come un agglomerato di siti web indipendenti tra loro, ma va considerato come l'insieme delle capacità tecnologiche raggiunte dall'uomo nel campo della diffusione e della condivisione delle informazioni, e del sapere in generale. Possiamo guardare alla Rete come a un ambiente che permette di sperimentare nuove forme di contatto, di relazione e di espressione personale, quali i social network, che sono divenuti non semplici spiagge per turisti curiosi di passaggio, ma *habitat* in espansione[4].

I *digital media*, così, sono divenuti contesti di fruizione d'informazione, come spazi alternativi alla realtà quotidiana per momenti di sva-

[4] Nella letteratura italiana cfr. G.F. Ferrari, *Le libertà e i diritti*, in P. Carrozza, A. Di Giovine, G.F. Ferrari, *Diritto costituzionale comparato*, Roma-Bari, Laterza 2011; S. Bonfiglio, *Diritti fondamentali, territorio e partecipazione politica nella società della rete*, in F. Antonelli, E. Rossi (a cura di), *Homo Dignus. Cittadinanza democratica e diritti in un mondo in trasformazione*, Milano-Padova, Wolters Kluwer 2014.

Abstract

L'identità digitale: dalle nuove frontiere del Sistema Pubblico di Identificazione (SPID) alle problematiche legate al web

L'emergere del concetto di identità online ha generato un ampio dibattito nel mondo accademico. L'identità digitale può essere vista sotto un duplice aspetto. Da un lato le credenziali che ognuno possiede, e ciò trova il suo fondamento nel nuovissimo Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese (SPID). Dall'altro lato, l'identità digitale è la rappresentazione virtuale dell'identità reale, che può essere usata durante interazioni elettroniche con persone o macchine. L'identità è piuttosto mutevole, in continua evoluzione e trasformazione, sulla base delle esperienze che ogni individuo vive. In questo modo, il diritto all'identità personale implica una serie di corollari quali: il diritto a un nome, il diritto di replica, il diritto alla protezione dei dati personali e il diritto di un'immagine. Se traduciamo il diritto all'identità personale alla nostra epoca digitalizzata, con il suo uso massiccio dei social network, è necessario aggiungere al relativo decalogo dei diritti, il diritto all'oblio, ugualmente chiamato diritto di essere dimenticati. Sarà quindi possibile identificare le protezioni che le persone possono mettere in atto per difendere la propria identità e il diritto all'oblio.

Digital identity: from the new frontiers of SPID (Public System for the management of the Digital Identity of citizens and enterprises) to the world of the web

The emergence of the concept of online identity has generated much debate in the academic world. Digital identity can be seen in two ways. Firstly the credentials that everyone possesses and that has its foundation in the new Public System for Digital Identity management of citizens and businesses (SPID). On the other hand, the digital identity is the virtual representation of the real identity, which can be used during electronic interactions with people or machines. The identity itself is quite changeable, constantly evolving and transforming, based on the experiences that each individual lives. In this way, the right to personal identity implies a number of corollaries such as: the right to a name, the right of reply, the right to protection of personal data and the right to an image. If we translate the right to personal identity to our digitalized era, with its mas-

sive use of social networks, we need to add to the related decalogue of rights, the right to oblivion, equally called right to be forgotten. We will then identify protections that persons can put into place to defend their identity and the right to be forgotten.

Valentina Amenta,
Adriana Lazzaroni
Laura Abba

Ciberspazio e diritto, vol. 16, n. 52 (1-2015), pp. 29-50

Obblighi e responsabilità nell'utilizzo del documento informatico

Andrea Branca[1]

Sommario: 1. Premessa – 2. Documento informatico e firme elettroniche – 3. La responsabilità del certificatore – 3.1. Una disciplina generale per tutti i certificatori – 3.2. Una disciplina specifica per i certificatori qualificati – 3.3. Il regime delle responsabilità per i certificatori qualificati – 4. La responsabilità del titolare della firma – 5. La responsabilità dei destinatari del documento digitalmente sottoscritto – 6. Il regime delle responsabilità applicabile al caso di firma digitale apocrifa – 6.1. Uso del dispositivo da parte di terzi autorizzati dal titolare: il principio dell'apparenza imputabile – 6.2. Uso del dispositivo da parte di terzi, col consenso della controparte – 6.3. Uso del dispositivo da parte di terzi non autorizzati

1. Premessa

Con la recente pubblicazione del D.P.C.M. 13 novembre 2014[2] si arricchisce la serie di "Regole tecniche" dettate in materia di documento informatico. L'Esecutivo, infatti, dopo aver disciplinato le misure di sicurezza opportune nella gestione della posta elettronica certificata[3] e delle firme elettroniche[4], e dopo aver indicato le modalità operative di proto-

[1] Laureato in Giurisprudenza presso l'Università di Pisa. Si occupa di consulenza tributaria e assistenza ai contribuenti per l'Agenzia delle Entrate, Direzione regionale del Piemonte, Centro di Assistenza Multicanale di Torino. I contenuti e i pareri espressi nell'articolo sono da considerare opinioni personali dell'autore, che non impegnano in alcun modo l'Amministrazione di appartenenza.

[2] Il decreto è stato pubblicato sulla «Gazzetta Ufficiale» del 12 gennaio 2015 n. 8.

[3] D.P.C.M. 27 settembre 2012 ("Regole tecniche per l'identificazione, anche in via telematica, del titolare della casella di posta elettronica certificata").

[4] D.P.C.M. 22 febbraio 2013 ("Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali").

collazione[5] e conservazione[6] del documento informatico, si è ora occupato di "formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici".

La circostanza fornisce l'occasione per fare il punto sulle riflessioni finora condotte in materia di responsabilità dei soggetti coinvolti nell'utilizzo del documento informatico. Sarà quindi possibile proporre una sistematica visione del tema.

In questo approfondimento, dopo aver brevemente riassunto i punti salienti della materia [§ 2], osserveremo quali obblighi gravano sul certificatore della firma elettronica [§ 3], sul suo titolare [§ 4] ed anche sul destinatario del documento [§ 5]. Infine, analizzeremo il complesso intreccio d'interessi che si genera qualora il documento sia materialmente sottoscritto da un soggetto diverso da quello che ne appare l'autore [§ 6].

2. Documento informatico e firme elettroniche

Il D.Lgs. 7 marzo 2005 n. 82 ("Codice dell'amministrazione digitale" o "C.A.D.") è la principale fonte normativa in materia di documento informatico, definito «rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti»[7]. Tale strumento, com'è noto, non sempre può essere considerato una scrittura: è il giudice che valuta di volta in volta, sulla base del suo prudente apprezzamento[8]. Ma la società ha bisogno di certezze, deve sapere già nel momento in cui i negozi vengono documentati se la forma prescelta sia idonea allo scopo, senza attendere un'eventuale ed aleatoria decisione giudiziale. Questo è il ruolo della "firma elettronica", «insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica»[9]. Di questo *genus* esistono varie *species*

[5] D.P.C.M. 3 dicembre 2013 ("Regole tecniche per il protocollo informatico").

[6] D.P.C.M. 3 dicembre 2013 ("Regole tecniche in materia di sistema di conservazione").

[7] Articolo 1 comma 1 lettera p) del C.A.D.

[8] «L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità» (articolo 20 comma 1-*bis* del C.A.D.).

[9] Articolo 1 comma 1 lettera q) del C.A.D.

Abstract

Obblighi e responsabilità nell'utilizzo del documento informatico

L'articolo fa il punto sulle riflessioni finora condotte in materia di responsabilità dei soggetti coinvolti nell'utilizzo del documento informatico, proponendo una sistematica visione del tema. Dopo aver brevemente riassunto i punti salienti della materia, il testo esamina gli obblighi che gravano sul certificatore della firma elettronica, sul suo titolare e anche sul destinatario del documento. Infine, analizza il complesso intreccio di interessi che si genera qualora il documento sia materialmente sottoscritto da un soggetto diverso dall'autore apparente.

Duties and Liability in the use of Electronic Documents

This article focuses on the reflections carried out so far on the liability of those involved in the use of electronic documents, proposing a methodical vision of the theme. Having briefly summarized the main points of the subject, the text examines the obligations which affect the certification authority, the owner of an electronic signature and also the receiver of an electronic document. Finally, it analyses the complex intersection of interests that is generated when the document is physically signed by a person other than the apparent author.

Andrea Branca

Ciberspazio e diritto, vol. 16, n. 52 (1-2015), pp. 51-84

Informazione online, sequestro e responsabilità

Silvia Martinelli

Sommario: 1. Introduzione – 2. L'articolo 21 della Costituzione: nozioni introduttive – 3. Libertà di stampa e sequestro – 4. La nozione di stampa: primi cenni – 5. Web e sequestro: peculiari modalità – 6. Informazione online, nozione di "stampa" e sequestro – 7. Nozione di stampa e obbligo di registrazione – 8. Informazione online e responsabilità del provider – 9. Informazione online e responsabilità del direttore del giornale telematico nella sentenza della Cassazione n. 35511 del 2010 – 10. La nozione di stampa nella sentenza della Cassazione n. 10594 del 5 novembre 2013 – 11. La recentissima pronuncia delle Sezioni Unite

1. Introduzione

L'avvento del digitale, la creazione del World Wide Web e la sempre maggior diffusione delle nuove tecnologie hanno modificato il nostro modo di comunicare generando radicali trasformazioni all'interno della nostra società, tanto dirompenti da spingere gli studiosi a parlare di una nuova rivoluzione industriale e a coniare il termine "società dell'informazione".

Con tale locuzione, di origine incerta e risalente alla metà degli anni Sessanta, si definisce, generalmente, una società nella quale l'informazione ha assunto un ruolo centrale nello sviluppo delle attività umane, anche in termini di risorse economiche generate, subentrando in questo ruolo all'industria[1].

La diffusione delle telecomunicazioni, con la televisione in ogni casa, costituisce una prima rivoluzione che ha interessato il nostro modo di comunicare, di informarci e di fare informazione, a cui è seguito l'avvento del World Wide Web, la diffusione del computer in ogni casa, con

[1] Cfr. AA.VV., *Lessico del XXI secolo L-Z*, Treccani 2013.

la possibilità di comunicare ad un pubblico vasto e sconfinato, con immediatezza e a costi accessibili pressoché a tutti.

Le tecnologie *mobile* hanno poi amplificato tale fenomeno consentendo l'accesso alle informazioni e la creazione di nuove fonti informative in ogni momento della giornata, da ogni luogo, tramite un dispositivo potenzialmente sempre con noi.

In tale contesto, in continuo mutamento, occorre riflettere sui concetti di libera manifestazione del pensiero, di stampa e di informazione, nel nostro ordinamento ancora ancorati alle disposizioni costituzionali e alla legge sulla stampa del '48.

2. L'articolo 21 della Costituzione: nozioni introduttive

L'articolo 21 della nostra Costituzione afferma, al primo comma, che «tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione». La lungimiranza dei Padri Costituenti ha consentito l'applicazione del diritto così proclamato anche a mezzi di diffusione dell'informazione e del pensiero che, al tempo, non erano ancora immaginabili.

Maggiori problemi interpretativi suscitano, invece, i successivi commi, nei quali il riferimento è limitato al concetto di stampa, la cui definizione è, tutt'oggi, controversa:

«La stampa non può essere soggetta ad autorizzazioni o censure.
Si può procedere a sequestro soltanto per atto motivato dell'autorità giudiziaria nel caso di delitti, per i quali la legge sulla stampa espressamente lo autorizzi, o nel caso di violazione delle norme che la legge stessa prescriva per l'indicazione dei responsabili.
In tali casi, quando vi sia assoluta urgenza e non sia possibile il tempestivo intervento dell'autorità giudiziaria, il sequestro della stampa periodica può essere eseguito da ufficiali di polizia giudiziaria, che devono immediatamente, e non mai oltre le ventiquattro ore, fare denunzia all'autorità giudiziaria. Se questa non lo convalida nelle ventiquattro ore successive, il sequestro s'intende revocato e privo di ogni effetto.
La legge può stabilire, con norme di carattere generale, che siano resi noti i mezzi di finanziamento della stampa periodica».

Abstract

Informazione online, sequestro e responsabilità

La stampa gode di una tutela rafforzata rispetto alle altre forme di manifestazione del pensiero. Essa, infatti, non può essere soggetta ad autorizzazioni o censure e il sequestro degli stampati è possibile solo secondo le modalità e con le limitazioni stabilite, in primo luogo, dalla stessa Costituzione. Il presente articolo affronta la questione dell'applicabilità della disciplina di cui all'art. 21 Cost. prevista per la stampa all'informazione diffusa online. Riflettendo sulla natura e sulle caratteristiche dei nuovi strumenti dell'informazione e sulla disciplina ad essi applicabile, mediante un'analisi della normativa vigente e delle pronunce della Corte di Cassazione in materia, sono analizzate le questioni relative alla definizione di "stampa", all'applicabilità del sequestro preventivo e dell'obbligo di registrazione della testata, nonché i profili concernenti la responsabilità, con riferimento sia alla responsabilità del direttore che alla responsabilità del provider.

Online media law, website blocking orders and responsibilities

Italian freedom of speech law is more favourable for traditional press than for online media. The traditional press cannot be object of authorizations or censorships and requisitions are possible if and only if terms and conditions fixed by Italian Constitution are respected. The present paper analyze the art. 21 of Italian Constitution and discuss his applicability to the online media, having regard to the law, the most important judicial opinions of Corte di Cassazione and the peculiarity of online communications. In order to clarify this core issue, the present paper focus on definition of press, website blocking orders, press registration and head editor and provider responsibilities.

Silvia Martinelli

Ciberspazio e diritto, vol. 16, n. 52 (1-2015), pp. 87-110

La sentenza "Google Spain" e l'interpretazione del diritto: alcune considerazioni

Luca Pelliccioli

Sommario: 1. Introduzione – 2. Sulla responsabilità dei gestori di motori di ricerca – 3. La creazione del diritto all'oblio – 4. La questione del bilanciamento

1. Introduzione

Spesso gli storici del diritto osservano che la tradizione giuridica dell'Occidente moderno si è costruita in opposizione al proliferare di diritti particolari che aveva caratterizzato l'età medievale. Un momento di emancipazione da quella condizione deplorevole fu la generale affermazione del concetto di norma giuridica come prescrizione generale e astratta. Le prescrizioni generali non riguardano casi o insiemi di casi particolari e individuati, ma classi di casi[1]; l'impero delle norme generali è dunque un rimedio al particolarismo di altre esperienze giuridiche. Non sempre, tuttavia, la generalità è un bene. A volte il diritto cade nel difetto opposto al particolarismo, allorché descrive classi di fattispecie troppo ampie; quando, in altre parole, le norme diventano *troppo* generali.

Anche se questo è un modo assolutamente comune di apprezzare e criticare la generalità delle norme giuridiche, si noti, esso confonde e mescola due diversi nozioni di generalità: la prima consistente nel riferimento a classi (universali) anziché a individui; la seconda da identificare con l'ampiezza del campo di applicazione. Quando si elogia la generalità delle norme giuridiche si presuppone verosimilmente un amalgama di queste due caratteristiche distinte. Una norma, per contro, non può essere *troppo* generale nel primo senso (non essendo l'universalità una grandezza scalare), ma solo nel secondo.

[1] Cfr. R. Guastini, *La sintassi del diritto*, Torino, Giappichelli 2011, p. 46.

Si è scritto che la disciplina italiana della protezione dei dati personali presenta in misura notevole il vizio di avere un campo di applicazione esageratamente ampio[2]. Sotto la lente del critico cadono diverse definizioni del decreto legislativo 196/2003 (e in precedenza della legge 675/96), come le definizioni di *dato personale* o di *trattamento*, tanto generali da attribuire a questa disciplina un campo di applicazione irragionevolmente esteso. Con la conseguenza, peraltro, di generare innumerevoli conflitti potenziali con altre parti del diritto che richiedono il ricorso a strumenti argomentativi che attribuiscono all'interprete un ineliminabile discrezionalità.

La recente e discussa sentenza C 131/12 del 13 maggio 2014 della Corte di giustizia UE è un buon banco di prova per queste considerazioni critiche non solo perché si occupa dell'interpretazione di alcuni articoli della direttiva UE 95/46 (d'ora in poi *la direttiva*) da cui derivano le definizioni estremamente generali sopra citate, ma anche perché offre di essi una interpretazione ampia, in una maniera certo inconsueta (e per qualcuno inattesa), eppure legittimata dal loro lasco e comprensivo tenore letterale[3].

Avrei detto: la recente e discussa sentenza sul diritto all'oblio, ma si dà il caso che un primo oggetto di controversia attenga proprio alla categoria giuridica alla quale ascrivere la decisione dei giudici di Lussemburgo. Mentre la maggior parte dei commentatori ammette infatti che tale sentenza (che ha ritenuto fondata la richiesta di un cittadino spagnolo di eliminare dall'indice del motore di ricerca Google Search alcuni dati relativi a una vecchia procedura esecutiva che lo aveva riguardato) abbia dato un importante impulso al riconoscimento del diritto all'oblio in ambito europeo, altri invece discutono l'adeguatezza di questa etichetta[4].

[2] Cfr. M. Jori, "Libertà di parola e protezione dei dati", «Ragion pratica», n. 12, 1999, pp. 109 e ss.

[3] Si veda A. Palmieri, R. Pardolesi, "Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google", «Nuovi Quaderni del Foro italiano», n. 1, 2014, p. 1 ss. Gli autori parlano di una scelta di sconfessare i precedenti «sforzi ermeneutici volti a contenere la portata espansiva insita in alcuni concetti chiave della direttiva». Sugli sforzi, paralleli, della prima "giurisprudenza" del Garante italiano della privacy vedi M. Jori, "Libertà di parola e protezione dei dati", cit.

[4] Cfr. P. De Hert, V. Papakonstantinou, "How the European Google Decision May Have Nothing To Do With a Right to Be Forgotten", *Privacy Perspectives*

Abstract

La sentenza "Google Spain" e l'interpretazione del diritto: alcune considerazioni

Questo articolo prende in considerazione i principali passaggi argomentativi della sentenza resa dalla Corte di giustizia UE nella causa C 131/12 (meglio nota come Google Spain). Ci si sofferma in particolare su tre aspetti della sentenza. In primo luogo, si sostiene, la scelta della corte di trattare il gestore di un motore di ricerca come responsabile del trattamento dei dati che vengono visualizzati in risposta a una ricerca è forse in contrasto con un orientamento consolidato, ma è senz'altro conforme alla lettera della Direttiva 95/46. In secondo luogo, tuttavia, con riguardo all'esistenza di un diritto all'oblio, la corte prende una direzione completamente diversa, non letteralista, rispondendo affermativamente e riconoscendo un diritto che in precedenza non faceva parte dell'ordinamento europeo. Più precisamente si tratta del diritto alla cancellazione di dati personali (o, meglio, dei link a siti contenenti tali dati) in seguito al (mero) trascorrere del tempo. Infine si sofferma l'attenzione sul bilanciamento tra diritto all'oblio (e, più in generale, alla privacy) e libertà di espressione; in questa sezione si cerca di mostrare che i giudici parlano in modo fuorviante di ponderazione tra privacy e "interessi" di vario tipo, trascurando pressoché completamente, o negando implicitamente, la rilevanza della libertà di parola e di informazione.

The "Google Spain" Judgment and the Interpretation of Law: Some Remarks

This article examines the main argumentative steps of the judgment given by the EU Court of justice in case C 131/12 (better known as Google Spain). Three topics of the decision receive special attention. First, it is argued, the court's choice to treat search engines service providers as controllers of the data shown as query results may be at odds with a strong tendency in the opposite direction, but it undoubtedly fits the literal meaning of the provisions of Directive 95/46. In the second place, however, with regards to the issue of the existence of a right to be forgotten the court takes a completely different, non literalist, route and answers in the affirmative recognizing a right that wasn't previously part of the european legal system. More precisely this is the right to have one's personal data (or, better, links to sites containig those data) erased due (solely) to the passing of time. Lastly, focus is placed on the balancing between the right to be forgottene (and, more generally, to privacy) and freedom of speech; this section tries

to demonstrate that judges misleadingly speak of the task of weighing privacy against "interests" of various kinds, almost entirely overlooking, or denying, the relevance of freedom of speech and information.

Luca Pelliccioli

Ciberspazio e diritto, vol. 16, n. 52 (1-2015), pp. 113-153

Libertà d'espressione in rete e tutela penale della reputazione digitale

Donato La Muscatella[1]

Sommario: 1. Comunicare globalmente: nuove opportunità e nuovi rischi – 2. La libertà di manifestazione del pensiero. Uno sguardo d'insieme – 3. La reputazione nel XXI secolo – 4. L'accertamento del fatto – 5. Le misure di cautela – 6. Quali prospettive di sviluppo per l'agorà digitale?

1. Comunicare globalmente: nuove opportunità e nuovi rischi

L'apertura dei fronti moderni della comunicazione ha sancito, con gli anni, inedite dimensioni espressive. Ciascuno conquista altre realtà, acquisendo una vera e propria identità digitale, non solo sociale in senso stretto, tanto da essere utilizzata anche da molte aziende per la selezione delle nuove risorse[2].

Riflessioni, critiche, opinioni, in una parola "messaggi" viaggiano in tempo reale da un capo all'altro del Globo, proponendo continui spunti di discussione.

L'evoluzione spaziale dei luoghi di confronto, tuttavia, è uno stadio di sviluppo comunicativo non privo di rischi.

Gli abusi – tanto quanto le potenzialità – di tali strumenti, aumentano giorno per giorno e quasi mai procedono in parallelo con la consapevolezza degli utenti (e del Parlamento).

A ciò s'aggiunga che, talvolta, produrre il maggior danno possibile è l'intenzione precipua di chi "sfrutta il Web".

I cc.dd. *discorsi di odio*, prima riservati ad alcuni luoghi di incontro virtuale – comunità e forum ideologizzati – sono ora ben più diffusi, avendo conquistato una fetta importante delle tematiche discusse sui social network.

[1] Avvocato in Ferrara, Perfezionato in *Computer Forensics* e Investigazioni Digitali presso l'Università degli Studi di Milano.

[2] Come evidenziato già nel rapporto LabItalia del 2012 (cfr. http://www.rassegna.it/ articoli/2012/02/15/83578/social-network-37-aziende-li-usa-per-selezione-personale).

Al di là della percezione di questi comportamenti, poi, il peso che tali condotte ha acquistato nel corso del tempo ha spinto gli interpreti ad occuparsene, tentandone un'approssimativa definizione.

Da questo punto di vista, può citarsi il Consiglio d'Europa, che, con nozione decisamente omnicomprensiva, li qualifica come discorsi che coprono ogni forma di espressione che diffonda, inciti, promuova o giustifichi odio razziale, xenofobia, antisemitismo o altre forme di odio basate sull'intolleranza, espressa con aggressivo nazionalismo ed etnocentrismo, discriminazione ed ostilità contro le minoranze, i migranti ed i popoli di origine immigrata[3].

Più settoriale la definizione adottata oltreoceano, che qualifica tali i «discorsi che attaccano una persona o un gruppo sulla base, ad esempio, della razza, della religione, del genere, della disabilità o dell'orientamento sessuale»[4].

L'interesse generale per il tema è testimoniato dalla nascita di campagne istituzionali che si propongono, tra l'altro, di «ridurre il livello d'accettazione di simili espressioni online, incrementare la consapevolezza dei rischi che generano, supportare e dimostrare solidarietà alla gente ed ai gruppi presi di mira, difendere lo sviluppo di consenso agli strumenti di politica europea che le contrastano e sviluppare la partecipazione e la cittadinanza dei giovani, anche nel governo delle dinamiche del Web».

Si tratta, tuttavia, di aggressioni che non trovano ancora ottimale regolamentazione – se si esclude il tentativo, pur apprezzabile, di estendere e rinnovare l'operatività della scarsamente applicata "legge Mancino"[5] – nell'ordinamento nostrano.

[3] «Hate speech, as defined by the Council of Europe, covers all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin» (cfr. *No Hate Speech Movement*, http://www.nohatespeechmovement.org/).

[4] Dall'inglese «speech that attacks a person or group on the basis of e.g. race, religion, gender, disability, or sexual orientation», cfr. J.T. Nockleby, "Hate Speech," in *Encyclopedia of the American Constitution*, L.W. Levy and K.L. Karst edition, vol. 3, Detroit, 2000, pp. 1277-1279.

[5] Sul punto, in relazione al D.L. approvato dal Senato della Repubblica il 15 febbraio scorso, vd. D. Pulitanò, *Di fronte al negazionismo e al discorso d'odio*, in *Diritto Penale Contemporaneo* (http://www.penalecontemporaneo.it/), 16 marzo 2015.

Abstract

La libertà di espressione in Rete e la tutela penale della reputazione digitale

La disamina, dopo una breve introduzione sulle nuove forme di comunicazione globale – e sulle conseguenti distorsioni nell'utilizzo della Rete – approfondisce i rapporti tra libertà di espressione e protezione della reputazione digitale.
L'esame delle norme che fondano la protezione della libertà di manifestazione del pensiero, integrato dall'analisi delle caratteristiche strutturali della diffamazione tramite il Web e dei profili procedurali legati all'accertamento del reato, consente di tracciare le linee principali dell'auspicabile riforma della materia.

Freedom of expression on the Net and the protection of digital reputation given by the criminal justice system

The analysis, after a brief introduction on new forms of global communication – and the consequent distortions in the use of the Net – explores the relationship between freedom of expression and protection of digital reputation.
The examination of the rules that underpin the protection of freedom of expression, supplemented by an analysis of the structural characteristics of defamation on the Web and procedural aspects related to the establishment of the offense allows you to trace the main lines of eligible reform of the issue.

Donato La Muscatella

Ciberspazio e diritto, vol. 16, n. 52 (1-2015), pp. 155-192

Prevention and fight against cybercrime: the ILLBuster project

Andrea Rossetti, Roberta Casiraghi, Giuseppe Vaciago, Stefano Ricci, Edoardo Colzani

1. Introduction[1]

Recent statistics show that information security problems do not concern only big corporations, but they also affect everyday life of common users. Data provided in recent years by the European Cybercrime Center (EC3) of Europol show both the increase of the demand for illegal on line products, and of the ranks of criminals willing to satisfy them: drug traffic, extortion, blackmail, money laundering, trafficking, consumption of child pornography. There is no aspect of criminal life that could not be derived from or have branches over the net, and according

[1] A. Rossetti is the author of paragraph 1; R. Casiraghi is the author of paragraphs 2, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, G. Vaciago is the author of paragraphs 3, 3.1; S. Ricci and E. Colzani are the authors of paragraphs 4, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, E. Colzani is the author of paragraph 5, 5.1, 5.2, 5.3.

to the McAfee research that refers to 2013, it generates a profit of criminal activities up to 750 billion euro per year. The behavior of criminals changes as rapidly as the technology they use does; it is creative, able to take advantage not only of technological development, but also of regulatory gaps and inadequacy of legal procedures. Troels Ørting, EC3's director, during a press conference hold in Brussels at the beginning of 2014 with the former UE commissioner of Internal affairs, Cecilia Malmstrom, expressed his concern over increasing sophistication of malware and of sexual violence against minors, and reported growing globalization of criminal activity, development of malware for mobile phones, and interest of malefactors in data stored in the cloud.

An example of a tool developed with criminal intent is Fast Flux net: the main instrument used to compromise security of even experienced users. The existence of such tools is well-known to those who have been involved in computer security since 2006, but there has been growing interest in recent years since it has become the main instrument to understand data from ostensibly reliable sites. Fast flux domain name server (DNS) is a technique that can be used to prevent identification of IP address of groups of malignant servers. By exploiting the way the DNS works, the criminal creates a large botnet, with nodes that join and leave the network faster than the police detection system can trace. Fast flux DNS exploits how load balancing (the method for distributing workloads across multiple computing resources) is built into the DNS: it allows registration of a number of IP addresses with a single host name by the administrator, in this way he/she can distribute the traffic among many different servers; but usually the IP addresses associated with a host domain do not change very often, if at all.

It is their operation that allowed over time to develop systems that permit to detect uses of these tools and to automatically report their potential.

The ILLbuster project deals exactly with this kind of tools: they have a preventive function, that is, they seek to act in order to prevent users' machines from being compromised; similar systems have been already partially-implemented in the antivirus that equips the most commonly used machines (and in the Italian legal system their use constitutes a legal requirement for those who process personal data). ILLBuster attempts to create preventive tools that work at the server level, and control dataflow.

Abstract

Prevention and fight against cybercrime: the ILLBuster project

The current paper offering an overview of the legal frameworks and requirements related to the ILLBuster Project. ILLBuster is a project funded by the European Commission (DG-HOME) within the programme "Prevention of and Fight against Crime". The goal of the project is to develop an integrated information system for the semi-automatic discovery of illegal activities over the Internet. The system is aimed to be a valuable tool to be used by LEAs for their activities of prevention of and fight against cyber-crime. The developed system will consist of the main engine aimed to detect and blacklist malicious internet domains.

Prevenzione e lotta contro la criminalità informatica: il progetto ILLBuster

Il presente lavoro offre una panoramica relative agli aspetti legali del progetto ILLBuster. ILLBuster è un progetto finanziato dalla Commissione Europea (DG-HOME) con il programma di "Prevenzione e Lotta al Crimine Informatico". L'obiettivo del progetto è quello di sviluppare un sistema per la scoperta semi-automatizzata di contenuti illegali in Rete. Il sistema è finalizzato a creare uno strumento di lavoro per le Forze dell'Ordine per svolgere le loro attività di prevenzione del crimine informatico. Lo sviluppo del sistema consiste nella creazione di un motore di ricerca in grado di individuare e inserire all'interno di una "blacklist" i domini malevoli presenti in Rete

Andrea Rossetti
Roberta Casiraghi
Giuseppe Vaciago
Stefano Ricci
Edoardo Colzani

Ciberspazio e diritto, vol. 16, n. 52 (1-2015), pp. 195-227

L'insostenibile leggerezza della proprietà industriale: gli *spaghetti description* dell'informatica forense nel processo

Donato Eugenio Caccavella

Un fenomeno che con sempre maggiore frequenza sta diventando oggetto di controversie giudiziarie consiste nella denuncia di sottrazione di dati rilevanti in termini di proprietà intellettuale ad opera di aziende concorrenti le quali, spesso attraverso collaboratori infedeli o con veri e propri accessi abusivi ad altrui sistemi informatici, riescono a acquisire documentazione riservata, fra cui, a titolo esemplificativo: documentazione di progetto; documenti commerciali; banche dati utilizzate per erogare servizi; contratti o listini prezzi dei fornitori; contratti o listini prezzi dei clienti della azienda titolare di tali dati.

È infatti intuibile che il possesso e il conseguente utilizzo di tali dati fornisce un rilevante e illegittimo vantaggio competitivo per l'azienda concorrente, potendo questa sfruttare le informazioni acquisite calibrando efficacemente la propria offerta in danno di quanto elaborerà il competitor – di cui può ragionevolmente conoscere la proposta commerciale – ovvero, in alternativa, parassitariamente usufruendo di informazioni e dati che l'azienda titolare ha probabilmente impiegato anni e costi per acquisire e consolidare.

Considerato che il "bene" illegittimamente acquisito consiste in documenti o dati informatici riversati da un sistema informatico a uno o a più sistemi informatici, l'acquisizione di tali reperti rientra pacificamente nell'ambito dell'informatica forense.

A fronte di tali condotte, per tutelare i propri diritti, l'azienda titolare può ricorrere in sede penale e/o civile in ragione delle contingenti e diverse esigenze sottostanti alle strategie giudiziarie da intraprendere.

Così definito l'argomento che qui interessa, il presente studio si limiterà a esaminare gli aspetti tecnici che occorre analizzare nel momento in cui venga intrapresa la via giudiziaria civilistica: infatti, mentre nella sede penale l'attività di indagine, pur non soggiacendo esclusivamente all'iniziativa del Pubblico Ministero, nei fatti ne dipende in punto agli esiti, al medesimo organo pubblico essendo demandato l'esercizio dell'azione penale, in sede civile l'azienda che si ritenesse danneggiata dalla condotta di una propria concorrente, assumerebbe un ruolo attivo e principale nella richiesta di tutela dei propri diritti lesi.

Per chiarire i termini della questione, è sufficiente ricorrere a un caso esemplare, peraltro oltremodo diffuso nella prassi, in cui si realizza una illegittima sottrazione di documenti e dati informatici presenti su sistemi informatici della azienda titolare, per essere riversati su altri sistemi informatici di uno o più soggetti che intendono trarne vantaggio: in tale contesto, sui reperti informatici della azienda ritenutane illegittimo possessore sarà quindi necessaria l'esecuzione di accertamenti tecnici, i quali, riguardando sistemi informatici, implicano l'intervento dell''informatica forense[1].

Invocare l'ausilio dell'informatica forense in una controversia giudiziaria, tuttavia, implica risolverne preliminarmente l'insita criticità, consistente nell'elevata alterabilità e volatilità del dato informatico, soprattutto in un contesto in cui rilevanti elementi probatori risiedono su sistemi informatici quasi sempre nella totale disponibilità della parte che ha interesse a distruggerli, alterarli, o cancellarli.

Occorre pertanto illustrare e tenere nella dovuta considerazione alcuni elementi di informatica forense che, pur potendo apparire distanti dalla fattispecie considerata, sono al contrario basilari per una corretta disamina della questione.

[1] Cfr. C. Maioli, "Dar voce alle prove: elementi di informatica forense", in *Crimine virtuale, minaccia reale*, a cura di P. Pozzi, R. Masotti e M. Bozzetti, Milano, Franco Angeli 2004, pp. 69 e ss., in cui è rinvenibile una definizione di informatica forense alla stregua di una «disciplina che studia l'insieme delle attività che sono rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova», finalizzata a «conservare, identificare, acquisire, documentare e interpretare i dati presenti su un computer».

Abstract

L'insostenibile leggerezza della proprietà industriale: gli spaghetti description *dell'informatica forense nel processo*

La denuncia di sottrazione di dati rilevanti in termini di proprietà intellettuale ad opera di aziende concorrenti, per il tramite di collaboratori infedeli che riescono ad acquisire documentazione riservata, sta diventando oggetto di controversie giudiziarie con sempre maggiore frequenza. Considerato che il "bene" illegittimamente acquisito consiste in documenti o dati informatici riversati da un sistema informatico a un altro, l'acquisizione di tali reperti rientra pacificamente nell'ambito dell'informatica forense. Il presente studio esamina quindi gli aspetti tecnici, anche sotto il profilo delle operazioni da eseguire e delle *best practices* da osservare, che occorre considerare nel momento in cui è intrapresa la via giudiziaria civilistica da parte dell'azienda danneggiata. Infatti, invocare l'ausilio dell'informatica forense in una controversia giudiziaria implica risolverne preliminarmente l'insita criticità, consistente nell'elevata alterabilità e volatilità del dato informatico, soprattutto in un contesto in cui rilevanti elementi probatori risiedono su sistemi informatici quasi sempre nella totale disponibilità della parte che ha interesse a distruggerli, alterarli o cancellarli.

The Unbearable Lightness of Industrial Property: Spaghetti Digital *Forensics in Trial*

The claim of misappropriation of relevant intellectual property by competitors, through disloyal partners who manage to acquire confidential documents, is becoming more frequently the object of quarrel. Considering that the "asset" unlawfully acquired consists of documents or computer data poured from one computer system to another one, the acquisition of these findings fall peacefully as part of digital forensics. The present study therefore examines the technical aspects, also in terms of what to do and the best practices to be observed, which should be considered when it's taken to the Courts by the company statutory damaged. In fact, invoking the help of computer forensics in a legal dispute involves preliminarily solving of the inherent problems, consisting in the high perishability and volatility of digital datas, especially when relevant evidences reside on computer system often in a total availability of the party interested in destroying, altering, or deleting them.

Donato Eugenio Caccavella