Ciberspazio e diritto, vol. 15, n. 51 (2/3-2014), pp. 147-188

Diritto all'informazione, diritto d'autore, diritto alla privacy: né vincitori né vinti

Fernanda Faini[1]

Indice: 1. I diritti fondamentali della rete – 2. L'evoluzione del diritto all'informazione: la trasparenza delle istituzioni e l'apertura dei dati pubblici – 3. Il diritto d'autore online – 4. Il diritto alla protezione dei dati personali nell'era dei byte – 5. Né vincitori né vinti: il necessario bilanciamento tra i diritti della rete

1. I diritti fondamentali della rete

Le possibilità offerte dalle tecnologie dell'informazione e della comunicazione hanno inciso profondamente sull'individuo, che oggi si realizza anche per mezzo dei byte ed esplica molte sue azioni nel nuovo territorio globale della rete.

Condivisione, partecipazione, semplicità e immediatezza sono le chiavi di interpretazione dell'odierna società digitale, in cui si spezzano i vincoli geografici e temporali della realtà fisica, mutano profondamente i rapporti fra soggetti e prendono forma nuove modalità di connessione e interazione. Internet da mero strumento di comunicazione diviene *agorà* in cui si sviluppa l'agire individuale, si intrecciano relazioni, si realizzano

[1] L'Autrice è laureata con lode in Giurisprudenza presso l'Università degli Studi di Firenze, ha conseguito il Master universitario di secondo livello in Management pubblico ed E-government presso l'Università del Salento ed è dottoranda in Scienze Giuridiche nel curriculum Diritto e nuove tecnologie presso l'Università di Bologna - CIRSFID. Responsabile dell'assistenza giuridica e normativa in materia di amministrazione digitale, innovazione, semplificazione, *open government* e sviluppo della società dell'informazione presso Regione Toscana. Collabora come docente in materia di diritto delle nuove tecnologie e amministrazione digitale con l'Università di Firenze, dove è cultore della materia "Informatica giuridica". Collabora come docente con Formez PA e altre realtà. Componente del Comitato di redazione della rivista scientifica «Ciberspazio e diritto» e della rivista «Il Documento Digitale». Autrice di pubblicazioni scientifiche e relatrice in convegni, seminari e conferenze in materia.

traffici giuridici, si incontrano opportunità e si devono prevenire e contrastare rischi e pericoli[2].

Tali caratteristiche sono amplificate nell'era del web 2.0, della multicanalità (pc, smartphone, tablet…), dei social media e delle applicazioni online (blog, forum, piattaforme di condivisione, social network, wiki…), delle app di messaggistica istantanea (come *WhatsApp*) e del *cloud computing*, costellazione di strumenti di una rete dinamica e interattiva, idonea a modificare il modo di intendere, utilizzare e condividere i contenuti e i dati. Il singolo diventa protagonista, autore e portatore di contributi: il web diventa testo "riscrivibile" da ciascuno, una grande piattaforma di condivisione, sviluppo e aggregazione di dati, informazioni, relazioni e servizi[3]. Le attività e il tempo della persona si spostano in rete, prendendo forma in strumenti diversi, ma connessi e "sincronizzati", che siano lo smartphone, il tablet, il pc: l'identità personale trova forma sempre più nella propria identità digitale.

Accanto alle molteplici opportunità, le rete rivela nuove problematiche, inediti rischi e pericoli per l'individuo. L'identità personale nella sua forma digitale, espressione dello stesso "io", necessita di un ripensamento. Nella rete, caratterizzata dalla condivisione, dall'ubiquità e dalla dinamicità, il soggetto conosce una nuova vulnerabilità e può trovarsi vittima di decontestualizzazioni, frammentazioni, violazioni e conseguenti danni[4].

La vita digitale, parte integrante della nostra esistenza, esige pertanto una particolare attenzione e la previsione di una conseguente adegua-

[2] In tal senso il volume del Garante per la protezione dei dati personali, *Educare alla rete. L'alfabeto della nuova cittadinanza nella società digitale*, 29 gennaio 2014 (doc. web n. 2893536, disponibile sul sito http://www.garanteprivacy.it, consultato il 30/11/2014).

[3] Cfr. G. Sartor, *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, 2ª edizione, Torino, Giappichelli 2010, in particolare p. 236 e ss.

[4] Nel web la dimensione informativa risulta dominante e può condurre ad una potenziale frammentazione dell'io in una pluralità di dati relativi al soggetto, con conseguenti possibili effetti lesivi e distorsivi ed eventuali fenomeni di decontestualizzazione. In tal senso C. Flick, *Privacy e legge penale nella società dell'informazione e della comunicazione*, in M. Cuniberti (a cura di), *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici*, Milano, Giuffrè editore 2008, p. 243 ss. e A. Mantelero, *Privacy digitale*, in M. Durante, U. Pagallo (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, UTET giuridica 2012, p. 159 ss.

Abstract

Diritto all'informazione, diritto d'autore, diritto alla privacy: né vincitori né vinti

Nella società attuale l'individuo si realizza anche per mezzo dei byte ed esplica molte sue azioni nell'*agorà* globale della rete. Il web offre molteplici opportunità, ma allo stesso tempo rivela nuove problematiche e inediti pericoli per l'individuo. Nella rete dinamica e interattiva, caratterizzata dalla condivisione, dall'ubiquità e dall'immediatezza, l'identità personale nella sua forma digitale, espressione dello stesso io, conosce una nuova vulnerabilità e può trovarsi vittima di decontestualizzazioni, frammentazioni, violazioni e conseguenti danni. L'identità digitale e i diritti che la connotano, pertanto, necessitano di una protezione adeguata alla realtà digitale.
Nell'affresco di diritti afferenti alla rete, sono degni di particolare attenzione il diritto all'informazione e alla conoscenza, il diritto alla privacy e il diritto d'autore, che sono stati fortemente investiti dall'evoluzione del web e che spesso si scontrano in rete. I conflitti chiamano in questione il diritto con la correlata necessità di stabilire le regole del gioco. Nella regolamentazione nascono, però, nuove problematiche, dal momento che è difficile stabilire una gerarchia fra diritti dotati di fondamento costituzionale. Si assiste, di conseguenza, al ricorso a soluzioni, che attribuiscono ad un'autorità o persino a un soggetto privato (Google) l'onere di gestire amministrativamente le questioni di conflitto. Resta il possibile ricorso all'autorità giudiziaria, ma questi soggetti assumono in concreto un ruolo centrale e sono essi stessi forieri di ulteriori e talvolta peggiori contrazioni dei diritti. È allora il caso di porsi una domanda: sono davvero in guerra questi diritti? In realtà il luogo di sintesi c'è ed è la persona e la sua identità digitale. Sotto tale chiave di lettura emergono i punti di convergenza e i nemici comuni e può essere intrapresa una nuova riflessione e una conseguente diversa regolamentazione, aderente alla realtà fatta di byte. Anche se è arduo tentare una soluzione a problematiche immanenti alla stessa vita digitale, la risposta può essere cercata in un ripensamento del presunto conflitto tra i diritti sotto il tetto dello stesso "io digitale" da proteggere. Senza bisogno di trovare né vincitori né vinti.

Right to information, copyright, right of privacy: no winners or loser

In today's society the individual can fulfil his needs also by means of bytes and performs many of his actions in the agora global network. The web offers many opportunities, but at the same time it reveals new problems and unknown dan-

gers to the individual. In the dynamic and interactive network, characterized by the sharing, ubiquity and immediacy, personal identity in its digital form knows a new vulnerability and may be the victim of decontextualization, fragmentations, violations and consequential damages. Digital identity and its new rights require adequate protection to the digital reality.

Among the rights of the web, special attention must be given to the right to information and knowledge, the right to privacy and copyright, which are heavily invested in the evolution of the web and that often clash with each other. These conflicts call into question the right with the related need to establish the rules of the game. However, new problems arise in the regulation, since it is difficult to establish a hierarchy of rights with constitutional basis. There is, therefore, the use of solutions, which attach to an administrative authority or even to a private party (Google) the burden of managing the issues of conflict. It remains possible to resort to the courts, but these subjects assume a central role in practice and are carriers of more and sometimes worst contractions rights.

It therefore seems necessary to ask a question: are these rights really at war with each other? Actually a place of synthesis exists and it is the person and its digital identity. Under this interpretation emerge the points of convergence and the common enemies, and we can take a new reflection and a consequent different regulation, adhering to the reality of bytes. Although it is difficult to attempt a solution to the problems inherent to the same digital life, the solution can be sought in a rethinking of the alleged conflict between the rights under the roof of the same "digital self" to be protected. No need to find neither winners nor losers.

Fernanda Faini

Ciberspazio e diritto, vol. 15, n. 51 (2/3-2014), pp. 189-204

Processo telematico e formalismo digitale alla vigilia dell'obbligatorietà del 31 dicembre 2014

Nicola Gargano

Indice: 1. L'obbligatorietà del deposito telematico e la fonte normativa – 2. 31 dicembre punto di partenza o punto di arrivo? – 3. L'atto telematico ed i suoi requisiti – 4. Gli errori più comuni nel deposito dell'atto ed eventuale rimessione in termini – 5. Il deposito telematico dell'atto introduttivo – 6. Conclusioni

1. L'obbligatorietà del deposito telematico e la fonte normativa

Il 31 dicembre 2014, l'obbligatorietà del deposito telematico degli atti sarà completa (o quasi). Scatterà infatti l'obbligo di deposito telematico previsto dall'art. 16bis del dl 179/2012, in tutte le procedure pendenti e per tutti gli atti depositati dalle parti già costituite.

Attualmente, dalla lettura dell'art. 16-bis del d.l. n. 179/2012, conv. con mod., in l. 221/2012, e ulteriormente modificato dal d.l. 90 del 24 giugno 2014, l'esclusività del deposito telematico non riguarda tutti gli atti del processo in tutti gli uffici giudiziari, ma è prevista esclusivamente per alcuni atti e precisamente per quelli relativi alle cause introdotte dopo il 30 giugno 2014, presso i tribunali e proposti dalle parti già costituite, per il ricorso per decreto ingiuntivo ed infine per tutti gli atti depositati dal professionista delegato nell'ambito di procedure concorsuali.

Menzione separata, sempre per quanto riguarda l'attuale vigenza, meritano le procedure esecutive il cui obbligo riguarda tutti gli atti successivi al primo atto con cui inizia l'esecuzione, ritenendosi però che tale obbligo non si applichi alle procedure di opposizione all'esecuzione che aprono un subprocedimento nuovo e con diverso numero di ruolo. Discutibile è invece l'applicabilità alle procedure di intervento nelle procedure esecutive dovendosi comunque subordinare l'obbligo di deposito telematico alla preventiva costituzione in giudizio della parte come espressamente previsto dal primo comma dell'art. 16 bis.

Ad ogni buon conto, si segnala che, per le procedure esecutive, per le quali è prevista l'applicazione delle nuove disposizioni del D.L. 132/2014,

e quindi iscrizione a ruolo con deposito in cancelleria di titolo esecutivo, verbale di pignoramento e/o atto di pignoramento a cura dell'avvocato, l'obbligo di iscrizione a ruolo telematica decorrerà dal 31 marzo 2015.

Il d.l. 90/2014 ha tuttavia rimodellato l'obbligo di deposito telematico, prevedendo una gradualità dell'entrata in vigore dell'obbligatorietà, che, tuttavia, rimarrà ancora esclusa per gli atti introduttivi e più in generale per gli atti delle parti non ancora costituite in giudizio.

Il 30 giugno 2014, infatti è entrata in vigore l'obbligatorietà del deposito telematico, solo relativamente al procedimento di ingiunzione – esclusa la fase di opposizione –, mentre, per le tipologie di atti sopra elencate, l'esclusività del deposito telematico si applica solo per le cause iscritte a ruolo dopo il 30 giugno 2014, rinviandosi l'obbligatorietà al 31 dicembre 2014 per tutti i giudizi in corso.

Di fatto, tale previsione di legge, costituisce una vera era e propria proroga, se si pensa che, iscrivendo una causa a ruolo dopo il 30 giugno e considerando la sospensione feriale, i primi atti in corso di causa andranno presumibilmente a scadere dopo il 31 dicembre 2014, termine fissato per tutte le cause in corso.

Si rammenta inoltre che l'obbligatorietà riguarderà solo i giudizi civili e di volontaria giurisdizione dinanzi ai Tribunali, poiché per le corti d'appello il termine dell'obbligatorietà è stato fissato per la data del 30 giugno 2015 (art. 16-quinquies).

Tuttavia, a partire dal 30 giugno 2014, è comunque possibile depositare con modalità telematica con valore legale e presso tutti i tribunali italiani, tutti gli atti previsti dalla legge come obbligatori.

2. 31 dicembre punto di partenza o punto di arrivo?

Ma il 31 dicembre può realmente considerarsi un traguardo? La seconda domanda che ci si deve porre per rispondere alla prima, è che fine abbia fatto il codice di procedura civile in un sistema regolato ormai da innumerevoli decreti legge più o meno coordinati tra loro, e che rinviano a loro volta a regole e specifiche tecniche riportate in decreti ministeriali o provvedimenti della DGSIA[1]. A ciò si aggiungono i numerosi

[1] D.G.S.I.A.: Direzione Generale dei Sistemi Informativi Automatizzati presso il Ministero della Giustizia.

Abstract

Processo telematico e formalismo digitale alla vigilia dell'obbligatorietà del 31 dicembre 2014

Il 31 dicembre 2014 è scattato l'obbligo di deposito telematico previsto dall'art. 16bis del dl 179/2012, in tutte le procedure pendenti e per tutti gli atti depositati dalle parti già costituite.
Ma il 31 dicembre può realmente considerarsi un traguardo? Per quando si descriverà nell'articolo che segue la normativa sul processo civile telematico, appare tutt'altro che chiara e trasparente rischiando, nella maggior parte dei casi di lasciare l'avvocato perso in amletici dubbi che spesso investono le stesse modalità di deposito degli atti.
Il presente articolo si pone l'obbiettivo di analizzare quei profili tecnico-giuridici che hanno portato alla nascita di una nuova figura giurisprudenziale, ovvero "il formalismo digitale".
Si commenteranno ordinanze di giudici di merito di Roma e Livorno che sanciscono l'inammissibilità del ricorso per ingiunzione depositato in via telematica, allegando come atto principale un documento in formato pdf immagine oppure contenente link ipertestuali ad elementi esterni.
Orientamenti, sconfessati dai Tribunali di Perugia, Vercelli e Verbania in opposti orientamenti, confermando la buona prassi di numerosi giudici italiani, che a fronte di ricorsi per decreti ingiuntivi presentati in formato pdf immagine, invitavano semplicemente il ricorrente a ridepositare mediante busta integrativa l'atto nel formato corretto.
Si analizzeranno poi le problematiche relative agli eventuali errori effettuati nella compilazione della busta con le relative conseguenze e soluzioni, effettuando in conclusione una panoramica della giurisprudenza di merito sull'ammissibilità del deposito telematico di atti introduttivi e di costituzione in giudizio.

The electronic filing process and digital formalism on the eve of its compulsory application from 31 December 2014

The obligation for computerised filing provided for by art. 16 *bis* of Decree Law 179/2012 for all pending trials and for all documents filed by parties to civil proceedings came into force on 31 December 2014. However, can 31 December realistically be considered as a turning point? The legislation regarding the electronic filing process described in the following article appears to be less than

clear and transparent and risks, in many cases, generating Hamletesque doubts in the lawyer that often influence the means chosen for filing documents.
This article seeks to analyse the technical-legal issues that have led to the creation of a new jurisprudential phenomenon, that is, "digital formalism". Comments are given on rulings of merit pronounced in Rome and Livorno that confirm the inadmissibility of appeals for injunction filed electronically, with the attachment of a document image in pdf format or containing hyperlinks to external elements.
These guidelines have been contradicted by the Courts of Perugia, Vercelli and Verbania, which have taken an opposite view, confirming the correct practice of numerous Italian judges who, when dealing with petitions for injunctions submitted in pdf image form, simply invite the applicant to re-file the document in the correct format by means of an integrative attachment.
Problems relating to possible errors made in the compilation of the attachment with relative consequences and solutions are analysed; finally, an overview of jurisprudence regarding the admissibility of the electronic filing of introductory documents and of appearance before the court is given.

Nicola Gargano

Ciberspazio e diritto, vol. 15, n. 51 (2/3-2014), pp. 207-233

Privacy Protection, applicable Law and Jurisdiction Issues in Cloud Computing: an International and EU prospective.

Nadina Foggetti

Indice: 1. Introduzione – 2. Qualificazione dei contratti di cloud computing – 3. Legge applicabile e competenza giurisdizionale nel cloud computing – 4. La tutela della privacy nei servizi di cloud computing

1. Introduzione

Il *Cloud Computing* comprende un insieme di tecnologie che permettono, tipicamente sotto forma di un servizio offerto da un provider al cliente, di memorizzare/archiviare e/o elaborare dati (tramite CPU o software) grazie all'utilizzo di risorse hardware/software distribuite e virtualizzate in Rete in un'architettura tipica *client-server*. Una caratteristica del cloud computing è la delocalizzazione delle risorse utilizzate e messe a disposizione degli utenti. Il "cloud" rappresenta l'evoluzione naturale dei tradizionali *data centers*, poiché permette di mettere a disposizione risorse nell'ambito di *standards-based Web services* a fronte della sottoscrizione di *service-level agreements (SLA*) con un corrispettivo proporzionato all'effettivo utilizzo delle stesse. I servizi offerti sono comunemente indicati come *IaaS (Infrastructure as a Service), PaaS (Platform as a Service) e SaaS (Software as a Service)*.

I contratti di cloud computing pongono una serie di problemi in relazione alla qualificazione degli stessi in virtù di talune peculiarità che afferiscono all'aspetto squisitamente tecnico, ma che si riverberano inevitabilmente sul piano giuridico. Un primo profilo attiene alla natura ibrida del software costituito da un insieme di algoritmi (istruzioni in forma di processo immateriale), nonché dai mezzi materiali su cui queste istruzioni sono tradotte ed incorporate (dischi magnetici, CD). La complessità strutturale rende difficile la classificazione del software ponendo l'annosa questione giuridica relativa alla qualificazione dello stesso come pro-

dotto ovvero alla stregua di un servizio. Da un punto di vista giuridico, la qualificazione tecnica quale prodotto determina la qualificazione giuridica nell'ambito dei contratti di compravendita, la qualificazione tecnica quale servizio, comporta l'inquadramento nell'ambito delle norme che regolano ad esempio, l'appalto. Un ulteriore aspetto che occorre tenere in considerazione, afferisce all'inscindibilità nel cloud computing tra hardware e software. La macchina da sola, infatti, non è in grado di svolgere alcun compito da un canto e dall'altro gli stessi programmi non sono in grado da soli di fornire utilità, in assenza di determinate macchine. Da queste caratteristiche deriva quella che si definisce l'opacità dei contratti di questo tipo. Con tale termine si indica la difficoltà di individuare la singola responsabilità contrattuale nell'ipotesi di comportamento illecito di uno dei contraenti che non ottemperi agli obblighi previsti. Nell'ambito del cloud computing, infatti, è estremamente difficile ricondurre la responsabilità dell'evento dannoso in capo ad uno specifico contraente e quantificarne successivamente l'incidenza. Dalle problematiche individuate deriva, inevitabilmente l'atipicità standardizzata che è una caratteristica tipica dei contratti informatici e quindi anche di quelli aventi ad oggetto il cloud computing ed è determinata dall'estrema difficoltà di riferire un negozio avente ad oggetto hardware e software ad un preciso schema contrattuale tipico, in quanto la natura dei servizi erogati appare mista e disomogenea. Prima di analizzare le problematiche evidenziate, occorre rilevare che il presente studio si inquadra nell'attività di ricerca svolta a supporto del Progetto PRISMA. Un progetto di ricerca industriale finanziato dal PONREC, che coinvolge una partnership costituita da piccole e grandi aziende nazionali, autorevoli centri di ricerca e importanti università italiane, tra cui l'Università degli Studi di Bari A. Moro, l'Università di Catania, l'Università di Enna "Kore", l'Istituto Nazionale di Fisica Nucleare, il Consiglio Nazionale delle Ricerche, il CNR ISTC, SME del settore ed enti istituzionali quali *l'Innovapuglia*. Tutti i partner collaborano per fornire alle Smart Communities una soluzione sostenibile nel tempo e che abbia le caratteristiche tecniche per costituire un solido fondamento per lo sviluppo dell'Agenda Digitale Nazionale ed Europea. Obiettivo principale del progetto PRISMA è quello di dare vita ad un'innovativa piattaforma Open Source di cloud computing progettata per semplificare, migliorare e sviluppare nuovi processi per la Pubblica Amministrazione. Le attività di sperimentazione sono basate sulla Piat-

Abstract

Privacy Protection, applicable Law and Jurisdiction Issues in Cloud Computing: an International and EU prospective

Il *Cloud Computing* rappresenta l'evoluzione dei tradizionali *data centers*, poiché permette di mettere a disposizione risorse nell'ambito di *standards-based Web services* a fronte della sottoscrizione di *service-level agreements (SLA*) con un corrispettivo proporzionato all'effettivo utilizzo delle stesse. I servizi offerti sono comunemente indicati come *IaaS* (Infrastructure as a Service), *PaaS* (Platform as a Service) e *SaaS* (Software as a Service). A livello internazionale e nell'ambito dell'UE manca una disciplina uniforme del cloud computing. Pertanto la prima parte del paper si prefigge l'obiettivo di analizzare le problematiche connesse alla qualificazione dei contratti di cloud e i profili attinenti alla legge applicabile ed alla giurisdizione

La seconda parte del paper sarà incentrata sulle problematiche connesse alla data security ed alla privacy dei dati, che acquisiscono una specifica peculiarità nell'ambito dei servizi di cloud, in ragione della caratteristica della *multi-tenant* del cloud computing.

In conclusione si analizzeranno le prospettive future della disciplina del Cloud Computing anche alla luce della Proposta di Regolamento sulla protezione dei dati (Com 2012 11 def) che mira ad uniformare la disciplina del trattamento dei dati transfrontaliero negli Stati membri dell'Unione europea e negli Stati non membri, nonché l'emergente necessità di individuare standard internazionali e di elaborare una Convenzione internazionale sul cyber spazio che al momento non esiste.

Privacy Protection, applicable Law and Jurisdiction Issues in Cloud Computing: an International and EU prospective

Cloud Computing services are the natural evolution of traditional *data centers*, they are distinguished by exposing resources (computation, data/storage, and applications) as *standards-based Web services* and following a "utility" pricing model where customers are charged based on their utilization of computational resources, storage, and transfer of data. They offer subscription-based access to infrastructure, platforms, and applications that are popularly referred to as *IaaS* (Infrastructure as a Service), *PaaS* (Platform as a Service), and *SaaS* (Software as a Service).

At International and EU level there are not a uniform qualification and there are not a regulation concerning cloud computing. In the context of cloud computing it is necessary to define the qualification of cloud computing agreement and to analyse the issues concerning applicable law and jurisdiction. This analysis will be conduct in the light of Regulation Rome I and Rome II and also in the perspective of the recently Draft Report concerning Unleashing the potential of cloud computing in Europe (2013/2063(INI)).

The second part of this paper will concern the protection of privacy of cloud computing data. This issue is common to all typology of cloud computing services.

The content of data security and privacy protection in cloud is similar to that of traditional data security and privacy protection. It is also involved in every stage of the data life cycle. But because of openness and multi-tenant characteristic of the cloud, the content of data security and privacy protection in cloud has its particularities.

Finally the paper will analyse the future prospective also in the light of the Draft Proposal of Regulation regarding data protection (Com 2012 11 def) that aims to harmonize the legal framework regarding transnational data protection and the emerging issue regarding the elaboration of an International Convention regarding cyberspace that is lacking.

Nadina Foggetti

Ciberspazio e diritto, vol. 15, n. 51 (2/3-2014), pp. 235-269

L'avvocato e i servizi di *Cloud Data Storage*: privacy, responsabilità e doveri deontologici

Valerio Edoardo Vertua[1]

Indice: 1. Premessa – 2. Il quadro normativo di riferimento – 3. Le indicazioni del Garante Privacy – 4. Le Norme Deontologiche – 5. Il contratto con il *Cloud Service Provider* – 6. Le caratteristiche tecniche del Servizio di *Cloud Data Storage* – 7. Conclusioni

1. Premessa

L'avvocato, partner di uno studio associato, o forse ancor di più, singolo professionista, si avvale da tempo di servizi cloud: a volte in maniera inconsapevole, a volte consapevolmente ma con una certa disinvoltura, a volte ancora in maniera addirittura sconsiderata, senza verificare, aprioristicamente, la conformità delle proprie "scelte informatiche" alla luce delle vigenti normative, ivi comprese quelle deontologiche.

Tra i vari servizi cloud il professionista utilizza frequentemente quelli atti a memorizzare in remoto i propri dati ed i propri file (il c.d. *data storage*) e questo per svariati motivi: perché così abituato nella sua sfera personale/familiare oppure per precise scelte strategiche lavorative legate o alla gestione dei file in remoto o alla possibilità di sincronizzare i propri file in modo semplice ed efficiente tra i vari device – computer di ufficio/di casa, smartphone o tablet – oppure come unica modalità di backup oppure ancora quale componente di una politica di backup più complessa ed evoluta[2].

[1] Avvocato in Milano, perfezionato in Computer Forensics ed Investigazioni Digitali presso l'Università degli Studi di Milano, collaboratore della Cattedra di Informatica Giuridica ed Informatica Giuridica Avanzata della Facoltà di Giurisprudenza presso l'Università degli Studi di Milano; presidente dell'associazione DFA (Digital Forensics Alumni), co-fondatore e componente del Consiglio Direttivo con funzione di Coordinatore del Comitato Scientifico di Cloud Security Alliance Italy Chapter.

[2] Si desidera chiarire che, a parere di chi scrive, il *cloud data storage* rappresenta un'ottima ed efficiente opportunità di gestire anche da remoto i propri file incardinata

Nell'ambito di questo macro-sistema si è pensato di circoscrivere il presente studio alla figura del singolo avvocato, caratterizzato dalla necessità di un'efficiente organizzazione e da una capacità di spesa mediamente più limitata rispetto ai grandi Studi[3], che vuole impiegare nella sua attività professionale uno dei servizi di *cloud data storage* presenti sul mercato, operando una scelta consapevole alla luce: a) della vigente normativa sul trattamento dei dati personali – e quindi tutelando la privacy propria e dei propri clienti –, b) delle implicazioni di natura deontologica e c) di conseguenza delle eventuali sue responsabilità di natura civilistica e disciplinare.

In questo quadro si è pensato di usare come esempio il servizio di "Dropbox Pro"[4], un servizio quindi a pagamento basato sulla sincronizzazione di una cartella posta su uno o più device dell'utente (computer, smartphone o tablet) con un'analoga cartella su cloud. L'ottica di utilizzo del servizio è quindi basata sul fatto di avere una copia dei file anche, ma non solo, "in remoto" da affiancare alle normali politiche di backup adottate dal professionista. La scelta di usare come caso-studio questo *cloud provider* non è casuale bensì frutto di alcune sue precipue caratteristiche quali la semplicità di utilizzo, l'efficenza, la velocità di upload dei file in remoto, l'enorme diffusione e l'integrazione con numerose applicazioni software, soprattuto nell'ambito del mobile.

La presente analisi prende quindi le mosse dal quadro normativo di riferimento analizzando, seppure succintamente, le norme del c.d. Codice della Privacy (d.lgs. 196/2008) e le connesse norme civilistiche in materia di responsabilità che l'avvocato deve considerare nell'avvicinarsi ad un servizio cloud, verificando anche l'esistenza ed il contenuto di indicazioni specifiche del Garante della Privacy. Assumono poi una grande importanza nell'oggetto di questo scritto anche le norme deontologiche: si ritiene infatti che l'avvocato non possa, nella propria professione, considerare unicamente la dicotomia delineata dal c.d. Codice

però in un quadro più ampio di politica di backup; non si ritene infatti opportuno considerare il cloud come l'unica risorsa dove memorizzare i propri file.

[3] Fattore che può quindi condizionare fortemente anche la scelta dell'offerta contrattuale.

[4] Non si è potuto far riferimento alla tipologia "Dropbox for Business" perché le licenze minime da acquistare sono cinque e quindi al di fuori dei parametri che ci si è posti; cfr., https://www.dropbox.com/business (sito verificato il 15 novembre 2014).

Abstract

L'avvocato e i servizi di Cloud Data Storage*: privacy, responsabilità e doveri deontologici*

L'avvocato, partner di uno studio associato, o forse ancor di più, singolo professionista, si avvale da tempo di servizi cloud. Tra questi il professionista utilizza frequentemente quelli atti a memorizzare in remoto i propri dati ed i propri file (il c.d. data storage). Il presente studio è circoscritto proprio alla figura del singolo avvocato, caratterizzato dalla necessità di un'efficiente organizzazione e da una capacità di spesa mediamente più limitata rispetto ai grandi Studi (fattore che può quindi condizionare anche la scelta dell'offerta contrattuale), che vuole impiegare nella sua attività professionale uno dei servizi di cloud data storage presenti sul mercato. Al fine di permettere all'avvocato di operare una scelta consapevole, verranno presi in esame la vigente normativa sul trattamento dei dati personali – e quindi i principi atti a tutelare la privacy propria e dei propri clienti –, le implicazioni di natura deontologica, le eventuali responsabilità di natura civilistica e disciplinare, nonché le caratteristiche tecniche di uno dei primari e più diffusi servizi di cloud data storage preso ad esempio.

Lawyers and Cloud Data Storage *services: privacy, responsibility and deontological duties*

The lawyer, partner in a law Firm, or maybe even better, a single counsel, since long time is taking advantage of cloud services. Between the available services, the lawyer often make use of the ones useful to store in remote his own data and files (c.d. data storage). The present paper is limited to the person of the single lawyer, featured by the need of an efficient organization and by an expense capacity more limited compared to larger firms (influencing factor in a contract offer choice), who wants to expend in his practice one of cloud data storage services available in the market. In order to allow the lawyer to operate a conscious choice, this paper will take into consideration current legislation in processing personal data – and therefore the principles eligible to protect his own and his customers' privacy –, ethical nature implications, possible statutory and disciplinary liabilities and the technical features of one of the main and widespread cloud data storage services.

Valerio Edoardo Vertua

Ciberspazio e diritto, vol. 15, n. 51 (2/3-2014), pp. 273-309

Aspetti contrattuali del commercio elettronico: il contratto telematico e la disciplina del codice del consumo in materia di contratti a distanza alla luce delle recenti modifiche in vigore da giugno 2014

Silvia Martinelli

Indice: 1. Introduzione – 2. Il contratto telematico – 3. La manifestazione di volontà – 4. L'individuazione del momento in cui si verifica la conclusione del contratto – 5. Il luogo di conclusione del contratto – 6. Conclusione del contratto o conclusione dei contratti? – 7. La disciplina contrattuale ai sensi della Direttiva 31/2000 e del D.lgs. 70/2003 – 8. Il commercio elettronico B2C e il Codice del consumo – 9. La disciplina dei contratti conclusi a distanza – 10. Gli obblighi di informazione – 11. Il diritto di recesso – 12. La consegna del bene – 13. La legge applicabile, il foro competente, la tutela giurisdizionale e il ricorso stragiudiziale –14. Le principali novità introdotte dal D.lgs. n. 21 del 2014 in materia di contratti a distanza –15. La disciplina delle clausole vessatorie – 16. Conclusioni

1. Introduzione

In ambito economico, la digitalizzazione ha introdotto grandi trasformazioni, riducendo, se non persino eliminando, gli spazi e i tempi tipici del commercio tradizionale, e creando un mercato sempre più globale.

Lo scambio di beni e servizi che avviene attraverso un processo elettronico, il cosiddetto *e-commerce*, è stato oggetto di grande attenzione da parte del Legislatore comunitario sin dalla Comunicazione della Commissione europea n. 157 del 1997 ("Un'iniziativa europea in materia di commercio elettronico")[1], in quanto, oltre a costituire un settore decisivo per la crescita e la competitività futura, è un ottimo strumento per l'implementazione del mercato unico.

[1] Cfr. il documento COM(97) 157 - Un'iniziativa europea in materia di commercio elettronico. Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni 15/04/97.

Nella Comunicazione 157/1997 venne elaborata la distinzione tra "commercio elettronico diretto" e "commercio elettronico indiretto". Essa si basa su una distinzione sostanziale, in quanto il primo ha ad oggetto lo scambio di beni o servizi per i quali la conclusione del contratto avviene attraverso un processo telematico, mentre l'esecuzione avviene tramite i canali tradizionali, la posta e i vettori commerciali. Nel secondo, invece, anche l'esecuzione avviene attraverso la telematica. Ciò è possibile quando si tratti di beni digitali o digitalizzabili (ad esempio software, consulenze, e-book, musica).

Il Legislatore europeo ha disciplinato la materia con la Direttiva 2000/31/CE, nota come "Direttiva sul commercio elettronico" (Direttiva del Parlamento europeo e del Consiglio n. 31 dell'8 giugno 2000), relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico nel mercato interno.

Con riguardo al panorama normativo italiano, tali disposizioni sono state fedelmente recepite dal Legislatore nazionale con il Decreto Legislativo n. 70 del 2003, che costituisce la norma italiana di riferimento per il commercio elettronico.

Un'altra classificazione del commercio elettronico attiene, invece, ai soggetti coinvolti: commercio Business to Consumer (B2C), commercio Business to Business (B2B) e commercio Consumer to Consumer (C2C).

Si tratta di una classificazione fondamentale per quanto attiene alla disciplina contrattuale, poiché ai contratti conclusi tra un soggetto professionista e un consumatore sarà applicabile la dettagliata disciplina dei contratti a distanza prevista dal D.lgs. 205/2006, c.d. Codice del consumo.

Nel prosieguo saranno analizzati i principali aspetti contrattuali inerenti al commercio elettronico, con riferimento alla disciplina codicistica, alla Direttiva sul commercio elettronico e alla materia consumieristica.

2. Il contratto telematico

Il "contratto telematico" è comunemente definito come il contratto concluso a distanza mediante l'utilizzo della telematica. Si tratta, dunque, di un contratto che si distingue e caratterizza per le particolari modalità mediante le quali è concluso. Il mezzo utilizzato è lo strumento informatico e la conclusione avviene senza la presenza fisica delle parti contraenti.

Abstract

Aspetti contrattuali del commercio elettronico: il contratto telematico e la disciplina del codice del consumo in materia di contratti a distanza alla luce delle recenti modifiche in vigore da giugno 2014

L'articolo affronta i principali aspetti rilevanti in materia di contratti conclusi online. Lo scambio di beni e servizi che avviene attraverso un processo elettronico, il cosiddetto e-commerce, ha sollevato alcune importanti questioni interpretative in materia contrattuale, in particolare relativamente ai requisiti di forma e all'individuazione del momento e del luogo in cui si verifica la conclusione del contratto. La materia è stata disciplinata dalla Direttiva 31/2000, c.d. Direttiva sul commercio elettronico, recepita dal legislatore italiano con D.lgs. 70/2003, che stabilisce alcuni importanti obblighi per il soggetto prestatore, soprattutto in tema di trasparenza. La forma di commercio elettronico ad oggi più diffusa è quella che avviene tra un soggetto professionista e un soggetto consumatore. Per tale motivo è di fondamentale importanza per la materia de quo la disciplina contenuta nel Codice del consumo in materia di contratti conclusi a distanza, come modificata da ultimo con D.lgs. 21/2014, in vigore dal giugno 2014.

Contractual aspects of e-commerce: the online contract and Consumer Code regulation regarding contracts entered into at a distance, in the light of recent changes in force from June 2014

The article tackles the main aspects relating to contracts entered into online. The exchange of goods and services by electronic means, so-called e-commerce, has raised a number of important interpretative questions regarding contracts, particularly with relation to requirements of form and to the identification of the time and place that the contract is effectively entered into. The area is regulated by Directive 31/2000, the so-called e-commerce Directive, implemented by the Italian legislator with Leg. Dec. 70/2003, which establishes a number of important obligations for the provider of the service, especially with regards to transparency. The form of e-commerce most common today is between a professional person or entity and a consumer. For this reason, the regulations contained in the Consumer Code regarding contracts entered into at a distance, as recently amended with Leg. Dec. 21/2014, in force from June 2014, are of fundamental importance.

Silvia Martinelli

Ciberspazio e diritto, vol. 15, n. 51 (2/3-2014), pp. 313-340

La normativa italiana in materia di *whistleblowing*, *risk management* e *best practice* per la corretta gestione di un sistema di segnalazione

«*La disperazione più grave che possa impadronirsi di una società è il dubbio che vivere onestamente sia inutile*»

Corrado Alvaro

Alessandro Rodolfi

Indice: 1. Contesto normativo e spunti di miglioramento – 2. Piano Nazionale Anticorruzione, *risk management* e *whistleblowing* – 3. Ipotesi di un sistema di gestione per il *whistleblowing* – 4. Conclusioni

1. Contesto normativo e spunti di miglioramento

La promulgazione della Legge 6 novembre 2012, n. 190[1] recante le "*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione*" ha introdotto per la prima volta nel nostro Paese una norma specificamente volta alla regolamentazione giuridica del *whistleblowing*. La previsione di cui al punto 51 stabilisce che all'interno del decreto legislativo 30 marzo 2001, n. 165[2], sia inserito l'articolo 54-bis "*Tutela del dipendente pubblico che segnala illeciti*". Il legislatore, attraverso un iter deliberativo che ha visto il susseguirsi di diverse modifiche al testo nei lavori preparatori presso le Camere parlamentari, ha ritenuto di disciplinare la materia in un unico articolo composto da quattro commi:

[1] Si veda all'indirizzo http://www.funzionepubblica.gov.it/media/1037413/legge_6_novembre_2012_n_190.pdf (sito web consultato, e documento disponibile online, il 10 dicembre 2014).

[2] Il decreto legislativo in oggetto concerne le norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche; l'art. 54 bis si colloca sistematicamente nel Titolo IV concernete le regole del rapporto di lavoro e segue le previsioni del codice di cui all'art. 54.

«1. Fuori dei casi di responsabilità a titolo di calunnia o diffamazione, ovvero per lo stesso titolo ai sensi dell'articolo 2043 del codice civile, il pubblico dipendente che denuncia all'autorità giudiziaria o alla Corte dei conti, ovvero riferisce al proprio superiore gerarchico condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro, non può essere sanzionato, licenziato o sottoposto ad una misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia.

2. Nell'ambito del procedimento disciplinare, l'identità del segnalante non può essere rivelata, senza il suo consenso, sempre che la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione, l'identità può essere rivelata ove la sua conoscenza sia assolutamente indispensabile per la difesa dell'incolpato.

3. L'adozione di misure discriminatorie è segnalata al Dipartimento della funzione pubblica, per i provvedimenti di competenza, dall'interessato o dalle organizzazioni sindacali maggiormente rappresentative nell'amministrazione nella quale le stesse sono state poste in essere.

4. La denuncia è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni».

Prima di passare in rassegna, attraverso un'analisi critica, il contenuto dell'art. 54-bis è utile precisare che allo stato attuale non esistono norme di legge poste a tutela dei lavoratori che segnalano illeciti alle dipendenze di organizzazioni private ad eccezione di alcuni sistemi di controllo adottati da società di diritto italiano sottoposte alla "*Sarbanes Oxley Corporate Reform Act*" in ragione del fatto che le loro azioni sono quotate nel listino borsistico americano New York Stock Exchange[3]. Sorpren-

[3] In ragione della quotazione negli Stati Uniti, tali società sono soggette alle disposizioni della SOX che hanno influenza diretta sulla loro struttura di governance, in materia di controllo interno come stabilito dalle regole Securities and Exchange Commission (un ente di vigilanza federale statunitense simile alla Consob italiana). In particolare la sezione 301 della SOX prevede l'obbligo di adottare «procedure per la ricezione, l'archiviazione e il trattamento di denunce ricevute dalla società e riguardanti la tenuta della contabilità, i controlli contabili interni e la revisione contabile, nonché per la presentazione in via confidenziale o anche anonima di segnalazioni da parte di dipendenti in merito a pratiche contabili o di revisione censurabili».

Abstract

La normativa italiana in materia di whistleblowing, risk management *e* best practice *per la corretta gestione di un sistema di segnalazione*

Il termine anglossassone *whistleblowing* identifica l'istituto giuridico e le attività di regolamentazione volte a disciplinare le procedure che incentivano e proteggono le persone che segnalano illeciti oppure irregolarità. In Italia la "Tutela del dipendente pubblico che segnala illeciti" è stata recentemente introdotta dalla Legge n. 190/2012, che all'art. 54 bis reca le "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione". Partendo da un contesto più ampio, che obbliga ciascuna amministrazione pubblica a dotarsi di un Piano Nazionale Anticorruzione, il paper si propone di analizzare le modalità di funzionamento degli appositi canali utilizzati predisposti dalle organizzazioni per ricevere le segnalazioni. Tali Enti hanno iniziato a recepire pedissequamente il modello per la segnalazione delle condotte illecite pubblicato sul sito web del Ministero per la Semplificazione e la Pubblica Amministrazione ma pochi attualmente si sono adoperati per redigere ed implementare procedure specifiche tese a incentivare il fenomeno del whistleblowing. A tal fine si passeranno in rassegna alcuni esempi di concreta applicazione avviati sul territorio nazionale, evidenziando approcci seguiti ed eventuali spunti di miglioramento. Con lo scopo di supportare tali iniziative, Transparency International Italia, capitolo tricolore dell'Organizzazione non governativa leader mondiale nella lotta alla corruzione, ha lanciato un portale on-line destinato alla ricezione e alla gestione, in modo anonimo e protetto, delle segnalazioni di casi di corruzione. Il funzionamento del servizio web denominato "Allerta Anticorruzione - ALAC" concepito da TI-it e la sua esperienza maturata sul campo, offrono spunti interessanti per approfondire alcune materie trasversali al whistleblowing rappresentati dalle tematiche etiche e culturali, inerenti alla sicurezza informatica, alla privacy e all'anonimato.

Italian legislation with reference to whistleblowing, risk management, and best practices for the correct management of the reporting system

The Anglo-Saxon term *whistleblowing* refers to the legal concept and the regulatory activity aimed at governing the procedures that motivate and protect people that report illegal or irregular acts. In Italy, the "Protection of the public worker that reports illegal acts" was recently introduced by Law 190/2012, which under

art. 54 *bis* contains "provisions for the prevention and repression of corruption and illegality in the public administration". Starting from a wider context, which obliges every public administration to adopt a National Anticorruption Plan, the paper sets out to analyse how relevant channels are used by organisations to receive reports. These Bodies have begun to slavishly implement the model for reporting illicit conduct published on the Ministry for Simplification and Public Administration's website, but few are currently drawing up and implementing specific procedures aimed at motivating whistleblowing.
To this end, a number of examples of concrete application set up in Italy are reviewed, highlighting the approaches adopted and any areas for improvement. With the aim of supporting such initiatives, Transparency International Italia, the Italian branch of the non-governmental world leader in the fight against corruption, has launched an online portal for receiving and managing, in an anonymous and protected way, reports of cases of corruption. The web service called "Allerta Anticorruzione (Anti-corruption Alert) – ALAC" created by TI-it out of its experience gained in the field, offers interesting points of view from which to examine a number of transversal questions relating to whistleblowing, including ethical and cultural themes, and to I.T. security, privacy and anonymity.

Alessandro Rodolfi

Ciberspazio e diritto, vol. 15, n. 51 (2/3-2014), pp. 341-374

Riders on the storm: a radiograph of credit card fraud cases

Ioana Vasiu*, Lucian Vasiu

Contents: 1. Introduction – 2. – Legal elements – 2.1. Intent to defraud – 2.2. Access device – 2.3. Conspiracy and extraterritorial application – 3. Perpetration aspects – 3.1. Obtaining of card numbers – 3.2. Physical obtaining of cards – 3.3. Abuse of a position of trust – 4. Sentencing enhancements – 4.1. Amount of loss – 4.2. Number of victims – 4.3. Sophisticated means – 4.4. Role in the offense – 4.5. Upward adjustments – 5. Conclusion

1. Introduction

Credit card[1] remains a payment method widely used, despite the availability of a variety of electronic alternatives, such as digital wallets, checkout services, e-checks, or virtual currencies. In the United States ("U.S."), in 2012, the number of credit cards in force was about 333.6 million, the number of payments reaching 23.7 billion, for a total value of $2.2 trillion[2]. This impressive usage, however, presents abundant criminal opportunities.

The growing phenomenon of credit card fraud is a major concern for stakeholders, for a number of reasons. Credit card fraud losses can be up to 10 cents per $100 of the transaction value[3]. In the U.S., in 2012,

* Prof. Dr. I. Vasiu, Faculty of Law, Babeş-Bolyai University, *e-mail*: ioanav3@yahoo.com. This article is part of a large-scale research on computer crimes, including "Break on through: an analysis of computer damage cases", *Pittsburgh journal of technology law & policy*, vol. XIV, Spring 2014, pp. 158-201.

[1] "Credit card" is defined at 15 U.S.C. 1602(l) as «any card, plate, coupon book or other credit device existing for purpose of obtaining money, property, labor, or services on credit». "Credit" is defined at 15 U.S.C. § 1602(f) as «the right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment».

[2] Cfr. Federal Reserve System, *The 2013 Federal Reserve payments study*, July 2014, pp. 64-66.

[3] Cfr. J.S. Cheney et al., *The efficiency and integrity of payment card systems: industry views on the risks posed by data breaches*, 2012, p. 9.

the number of fraudulent transactions by credit card was 13.7 million, with a total value of $2.3 billion[4]. A high level of credit card fraud can impact negatively consumers' trust, an important social capital indicator[5] and a major factor in purchase intentions[6]. Particularly worrisome is the online victimization rate[7], as electronic commerce represents an increasing percentage of the overall trade[8], with credit card as an important method of payment[9]. Moreover, in certain massive breaches where credit card data was compromised, companies were sued by customers[10].

Financial gain is by far the most powerful motivation behind credit card frauds, however, these offenses can also be encountered as hacktivism, for instance the case where criminals used the credit card of a judge to purchase sex toys for him[11], or OpRobinHood, where members

[4] Cfr. Federal Reserve System, op. cit., p. 32.

[5] Cfr. L. Guiso, P. Sapienza, L. Zingales, "The role of social capital in financial development", «American economic review», vol. 94, n. 3, 2004, pp. 526-556.

[6] Cfr. C.-M. Chiu et al., "Understanding customers' repeat purchase intentions in B2C e-commerce: the roles of utilitarian value, hedonic value and perceived risk", «Information systems journal», vol. 24, 2014, pp. 85-114; Y. Fang, "Trust, satisfaction, and online repurchase intention: the moderating role of perceived effectiveness of e-commerce institutional mechanisms", «MIS quarterly», vol. 38, n. 2, 2014, pp. 407-427.

[7] Cfr. United Nations Office on Drugs and Crime, *Comprehensive study on cybercrime*, 2013, p. 25; CyberSource, *2012 Payments fraud survey*, 2012; LexisNexis, *Post-recession revenue growth hampered by fraud as all merchants face higher costs*, 2014.

[8] Cfr. U.S. Census Bureau, *Quarterly retail e-commerce sales 3rd quarter*, U.S. Department of Commerce, 2014.

[9] Cfr. J. de Lange, A. Longoni, A. Screpnic, *Online payments 2012: moving beyond the web*, 2012, www.ecommerce-europe.eu/stream/report-online-payments-2012, (20/11/2014); Civic Consulting, *Consumer market study on the functioning of e-commerce and Internet marketing and selling techniques in the retail of goods*, 2011, http://ec.europa.eu/consumers/archive/consumer_research/market_studies/docs/study_ecommerce_goods_en.pdf, (20/11/2014).

[10] Cfr. Remijas v. Neiman Marcus Group, LLC, No. 14 C 1735 (N.D. Ill. Sept. 16, 2014); Federal Trade Commission v. Wyndham Worldwide Corporation, n. 13-1887 (ES) (D.N.Y. Apr. 7, 2014); Consolidated Class Action Complaint, In re: Target Corporation Customer Data Security Breach Litigation, MDL No. 14-2522 (D. Minn Aug. 1, 2014), http://blogs.reuters.com/alison-frankel/files/2014/09/targetdatabreach-bankcomplaint.pdf, (12/11/2014); In re TJX Companies Retail Sec. Breach Litigation, 564 F.3d 489 (1st Cir. 2009).

[11] Cfr. L. Vaas, *Hacktivists use United States judge's credit card to buy sex toys for him*, http://nakedsecurity.sophos.com/tag/credit-card-fraud/, (6/7/2014).

Abstract

Riders on the storm: a radiograph of credit card fraud cases

Credit card frauds present an impressive array of forms and methods, often involving sophisticated means, organized crime aspects, and very significant criminal proceeds. Based on an extensive inquiry that involved the study of a large number of credit card fraud cases brought to the United States federal courts, press releases from law enforcement organizations, and information security reports, this article discusses the legal elements, the essential perpetration aspects, and the most relevant sentencing enhancements for these crimes, and proposes a number of improvements. The contributions of this article can be used for a more effective legal and judicial response, in the process of risk identification and mitigation, and for developing awareness and training programs. Although the article focuses on one jurisdiction, the findings, particularly those in the perpetration aspects section, and the conclusion would be useful to a global audience.

Riders on the Storm: una radiografia dei casi di frode relativi a carte di credito

Le frodi che riguardano le carte di credito sono contraddistinte da un'impressionante varietà di forme e metodi, che spesso implicano mezzi sofisticati, aspetti propri della criminalità organizzata, e azioni criminali piuttosto significative. Basato su una vasta indagine che ha incluso lo studio di un ampio numero di casi di frode relativi a carte di credito denunciati ai tribunali federali degli Stati Uniti, di comunicati stampa delle autorità di Pubblica Sicurezza, e di rapporti sulla sicurezza informatica, l'articolo esamina gli elementi giuridici, gli aspetti operativi fondamentali e i principali inasprimenti giudiziari relativi a tali crimini, proponendo alcuni miglioramenti. I contenuti dell'articolo si possono utilizzare per garantire una più efficace risposta legale e giudiziaria, nel processo di identificazione e attenuazione dei rischi, e nello sviluppo di programmi di formazione e divulgazione. Sebbene l'articolo si concentri su una giurisdizione specifica, i contenuti (in particolare quelli della sezione relativa agli aspetti operativi) e le conclusioni possono essere utili anche per un pubblico generale.

Ioana Vasiu
Lucian Vasiu

Ciberspazio e diritto, vol. 15, n. 51 (2/3-2014), pp. 375-411

Guida alla prova digitale: il primo approccio del Consiglio d'Europa all'armonizzazione delle diverse metodologie investigative

Mattia Epifani[1], Donato La Muscatella[2], Claudia Meda[3]

Indice: 1. La genesi della *Electronic Evidence Guide* – 2. La struttura del documento a) Fonti di prova; b) Perquisizione e sequestro; c) Acquisizione; d) Analisi; e) Preparazione e presentazione della prova; f) Giurisdizione; – 3. Il rischio degli standard in materia di prova scientifica – 4. Il tentativo europeo: pregi e difetti di uno strumento necessario

1. La genesi della Electronic Evidence Guide

Il crescente sviluppo delle tecnologie digitali e la diffusione di strumenti con la capacità di memorizzare dati come computer, smartphone e tablet sono divenuti causa e strumento utile a ricostruire fatti durante le attività investigative tanto di crimini informatici quanto di crimini comuni.

La possibilità di memorizzare dati su Cloud in modo semplice ed economico, inoltre, rende sempre più complessa la gestione ed il trattamento delle fonti di prova digitale da parte degli investigatori informatici.

Negli ultimi anni, poi, ha assunto sempre più importanza la necessità di definire e consolidare le metodologie di investigazione digitale, in modo da fornire conoscenze adeguate e multidisciplinari a tutte le figure

[1] CEO e Digital Forensics Analyst presso REALITY NET, Dottore in informatica e perfezionato in *Computer Forensics ed Investigazioni Digitali* presso l'Università degli Studi di Milano, certificazioni GCFA, GREM, GMOB, CEH, CHFI, CCE, CIFI.

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

[3] Laureata in *Ingegneria Elettronica* presso l'Università degli Studi di Genova, Dottoranda in *Scienze e Tecnologie per l'Ingegneria Elettronica e delle Telecomunicazioni* presso l'Università degli Studi di Genova.

professionali che interagiscono nella fase investigativa e nel procedimento giudiziario.

In questo scenario è nato e si è sviluppato, tra il 2010 e il 2013, il progetto di ricerca denominato *CyberCrime@IPA*[4], che ha visto la collaborazione di esperti provenienti da diversi Paesi appartenenti all'Unione Europea.

Lo studio aveva il duplice obiettivo di contrastare la criminalità informatica e di accrescere le competenze e le capacità delle Forze dell'Ordine, attraverso l'organizzazione di corsi di formazione multidisciplinari sulle tecniche di investigazioni digitali più comuni.

Sulla base di questi presupposti si proponeva, inoltre, di definire un protocollo per il trattamento delle fonti di prova digitale, al fine di fornire una visione complessiva dell'informatica forense ed una visione d'insieme delle problematiche relative alla gestione delle evidenze.

Tale guida, nota con il nome di *Electronic Evidence Guide*, aveva l'obiettivo di contribuire alla formazione di agenti di polizia, pubblici ministeri e giudici provenienti da diverse giurisdizioni. Come ben specificato all'inizio, lo scopo è quello di fornire un supporto per l'identificazione e la gestione di una prova digitale utilizzando metodi che garantiscano che sia garantita l'autenticità del reperto durante l'intero processo. («The purpose of the guide is to provide support and guidance in the identification and handling of electronic evidence using methods that will ensure that the authenticity of evidence will be maintained throughout the process»[5]).

A differenza di altri manuali che trattano argomenti analoghi, il documento si rivolgeva ad un ampio pubblico, comprendente non solo chi opera sul campo, come le forze dell'ordine, ma anche figure come giudici, pubblici ministeri, avvocati, notai e cancellieri, e si prefiggeva l'obiettivo di enucleare chiare direttive, dettando regole il più possibile

[4] Documento completo redatto da Nigel Jones, Esther George, Fredesvinda Insa Mérida, Uwe Rasmussen, Victor Völzow, consultabile, previa registrazione, all'indirizzo http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp.

[5] Vd. *Electronic Evidence Guide* – A basic guide for police officers, prosecutors and judges – Version 1.0, p. 7.

Abstract

Guida alla prova digitale: il primo approccio del Consiglio d'Europa all'armonizzazione delle diverse metodologie investigative

Il contributo esamina la Electronic Evidence Guide, primo risultato del lavoro del gruppo di esperti selezionati dal Council of Europe all'interno del progetto CyberCrime@IPA.
La Electronic Evidence Guide ha lo scopo di fornire supporto e linee guida per l'identificazione e la gestione delle fonti di prova digitale, illustrando metodi che garantiscano l'autenticità delle prove stesse durante tutto il processo. Pertanto, l'obiettivo della Guida è quello di costituire un documento che stabilisca i passi fondamentali di un'analisi forense, partendo dalla prima fase, costituita dalla definizione di fonte di prova digitale, passando per il tema della perquisizione e del sequestro, dell'acquisizione, dell'analisi, della preparazione e della presentazione della prova, per arrivare infine all'ultimo capitolo, dedicato agli aspetti più specificatamente legali.
Grazie all'iniziativa di tre associazioni (Digital Forensics Alumni, Tech and Law Center e DEFT Association) il documento è stato tradotto in lingua italiana, con il titolo "Guida alla prova digitale". Gli autori forniscono una panoramica sintetica ma completa della Guida, passando in rassegna la struttura e le diverse parti. L'analisi si conclude con la trattazione dei rischi di standardizzazione in materia di prova scientifica, tema in costante evoluzione, denunciando chiaramente i limiti ed i pregi di questo primo tentativo di armonizzazione delle indagini tecniche svolto a livello europeo.

Electronic Evidence Guide: first approach of the Council of Europe for he harmonization of different investigative methods

The paper examines the Electronic Evidence Guide, the first result of a research developed by a group of experts selected by the Council of Europe within the CyberCrime@IPA project.
The aim of the Electronic Evidence Guide is providing support and guidance for the identification and management of sources of digital evidence, showing methods guaranteeing both authenticity and integrity throughout the investigation process. Therefore, the purpose of the Guide is to provide a document that points out the basic steps of digital forensic analysis, defining the different source of digital evidence and explaining the seizure, acquisition, analysis, prep-

aration and presentation of the evidence. In the last chapter the guide deals also with legal aspects.
Thanks to the initiative of three associations (Digital Forensics Alumni, Tech and Law Center and DEFT Association) the Guide has been translated in Italian with the title "Guida alla prova digitale".
The authors provide a brief but suitable overview of the Guide, reviewing the structure and the different parts. The analysis ends with a discussion of the risks of standardization in the field of scientific evidence, clearly stating limits and worths of this first attempt at harmonization of technical investigations developed at European level.

Mattia Epifani
Donato La Muscatella
Claudia Meda

Ciberspazio e diritto, vol. 15, n. 51 (2/3-2014), pp. 413-452

Hate speech online: scenari, prospettive e criticità giuridiche del fenomeno

Francesco Di Tano[1]

Indice: 1. La società dell'informazione e la libertà di espressione – 2. Il c.d. *hate speech* – 3. Le principali forme di manifestazione di odio in Rete – 4. Lo scenario giuridico in materia di libertà di espressione. Il principio del danno e il principio di offesa (segue) – 5. Giurisprudenza e dottrina americana in tema di hate speech (segue) – 6. L'impostazione europea e il contesto italiano – 7. Le emergenti criticità giuridiche

1. La società dell'informazione e la libertà di espressione

Nel corso della storia, la comunicazione e l'informazione hanno rappresentato, per l'uomo e la società, preziose e ambite fonti di controllo sociale. Il potere sulle stesse, difatti, ha da sempre rappresentato il migliore collettore di consenso sociale, in grado di assicurare maggiore longevità al predominio di sistemi istituzionali rispetto al bieco utilizzo di forme di terrore o repressione[2].

Con l'avvento delle tecnologie digitali, tali aspetti si sono enormemente acuiti, avendo le stesse rivoluzionato le condizioni sociali nelle quali le persone comunicano e si esprimono e avendo consentito l'estensione dei mezzi di comunicazione a qualsiasi ambito della vita sociale, in una rete mutevole e dinamica, che è allo stesso tempo globale e locale, generica e personalizzabile[3]. Questo rilevante cambiamento ha portato alla ribalta fattori legati alla libertà di espressione che, pur essendo sempre esistiti, hanno catturato prepotentemente l'attenzione e le preoccupazioni degli studiosi e della società in generale[4].

[1] Avvocato del Foro di Reggio Emilia e Dottorando di ricerca in Diritto e Nuove Tecnologie presso il CIRSFID, Università di Bologna.

[2] Cfr. M. Castells, "Communication, Power and Counter-power in the Network Society", «International Journal of Communication», vol. 1, 2007, pp. 238-239.

[3] *Ivi*, p. 239.

[4] Cfr. J.M. Balkin, "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society", «New York University Law Review», vol. 79, n. 1, 2004, p. 2.

La rivoluzione digitale, infatti, ha ridisegnato i confini della libertà di espressione, alla stregua di quanto già fece in passato lo sviluppo delle tecnologie di radio e telecomunicazione. Essa ha consentito e consente tutt'ora la capillare e massiccia partecipazione culturale e la massima – per lo meno all'attuale stato della scienza e della tecnica – interazione umana e sociale[5]. Allo stesso tempo, però, ha comportato, quale altra faccia della medaglia, il sorgere di nuove opportunità per la limitazione e il controllo di tali forme di manifestazione sociale. Tutto ciò ha chiaramente reso essenziali e centrali le questioni inerenti alla libertà di espressione, inserita, mai come ora, nel contesto di quello che Castells definisce il reame dell'auto-comunicazione di massa[6].

La libertà di espressione rappresenta, difatti, uno dei temi tanto primari quanto controversi delle moderne società liberali, oggetto di ampi dibattiti in merito alla sua rilevanza, al suo bilanciamento con altri valori fondamentali e dunque alla sua limitazione e regolamentazione.

Tralasciando, in questa sede, le pur critiche ed estremamente rilevanti tensioni e contrapposizioni tra impresa, potere politico e utenti-utilizzatori di opere, l'interesse primario del presente contributo si volge a quegli aspetti della libertà di espressione (e della sua regolamentazione) che si rapportano con la dignità umana.

2. Il c.d. hate speech

Il fenomeno dell'*hate speech* è alimentato dall'impiego di epiteti discriminatori finalizzati all'insulto, all'offesa e alla stigmatizzazione di altri individui, sulla base della razza, del genere, dell'orientamento sessuale e di qualsiasi altra caratteristica o forma di appartenenza a gruppi.

Facendo propria la definizione adottata dal Consiglio d'Europa nel Protocollo Addizionale alla Convenzione sulla criminalità informatica sull'incriminazione di atti razzisti e xenofobici[7], per *hate speech* si intende "ogni materiale scritto, ogni immagine od ogni altra rappresentazione

[5] Cfr. J.M. Balkin, "The Future of Free Expression in a Digital Age", «Pepperdine Law Review», vol. 36, 2008, p. 112.

[6] Cfr. M. Castells, op. cit., pp. 246-259.

[7] http://conventions.coe.int/Treaty/EN/Treaties/Html/189.htm, (31.03.2014).

Abstract

Hate speech *online: scenari, prospettive e criticità giuridiche del fenomeno*

La rivoluzione digitale degli ultimi decenni ha ridisegnato i confini della libertà di espressione, favorendo la capillare e massiccia partecipazione culturale e la massima – per lo meno all'attuale stato della scienza e della tecnica – interazione umana e sociale, consentendo, però, allo stesso tempo, anche il sorgere di nuove opportunità per la limitazione e il controllo di tali forme di manifestazione sociale.
La libertà di espressione rappresenta uno dei temi più controversi delle moderne società liberali, oggetto di ampi dibattiti circa la sua rilevanza, il suo bilanciamento con altri valori fondamentali e dunque la sua limitazione e regolamentazione.
Ciò, specialmente laddove si prendano in considerazione quei comportamenti umani, di tipo espressivo, che sono diretti alla lesione del bene supremo della dignità dell'uomo.
Tra di essi, spicca il fenomeno dell'*hate speech*, che si estrinseca nell'impiego di epiteti discriminatori finalizzati all'insulto, all'offesa e alla stigmatizzazione di altri individui, sulla base della razza, del genere, dell'orientamento sessuale e di qualsiasi altra caratteristica o forma di appartenenza a gruppi.
L'articolo porta in evidenza il modo in cui le nuove tecnologie e soprattutto l'avvento di Internet abbiano influito sul fenomeno dell'*hate speech*, fornisce una panoramica sull'attuale dibattito dottrinario sulla regolamentazione dell'*hate speech* e il relativo scenario giuridico, che vedono contrapposte, da una parte, la visione statunitense, legata al Primo Emendamento, favorevole alla libertà di parola, dall'altra, la visione europea (e di altri Paesi), più attenta all'esigenza di proteggere i principi dell'uguaglianza e della dignità umana, anche a fronte della limitazione della libertà di manifestazione del pensiero. Analizza, altresì, le fattispecie più rilevanti, con le relative questioni giurisprudenziali, legate alle espressioni di odio nella Rete.
Infine, sono affrontate le maggiori criticità riguardanti l'*hate speech online*, connesse alla responsabilità degli Internet Service Providers e alla competenza giurisdizionale territoriale sui singoli casi (posto che l'assenza di confini su Internet impone proprio la necessità di ripensare i confini del diritto pubblico e privato online).

Hatespeech online: scenarios, perspectives and problematic juridical areas of the phenomenon

Digital revolution of the last decades has redrawn the boundaries of freedom of expression, encouraging widespread and massive cultural participation and the highest – at least in the current state of science and technology – human and social interaction, allowing, at the same time, even the arising of new opportunities for the limitation and control of these forms of expression in the society. In fact, freedom of expression is one of the most controversial issues of modern liberal societies, it is the subject of extensive debates about its relevance, its balance with other fundamental values and, therefore, its limitation and regulation. This, especially when you take into account those human expressive behaviours that are directed to the lesion of the supreme good of human dignity.
Among them, stands the *hate speech* phenomenon, which consists in discriminatory harassment, offences and stigmatizations of other individuals based on race, gender, sexual orientation and or any other characteristic or form of group membership.
This paper highlights how new technologies and especially the advent of the Internet influenced the hate speech phenomenon, and provides an overview of the doctrinal debate about the hate speech regulation and its related legal scenario, that see the counterposition, on the one hand, of the U.S. vision, linked to the First Amendment and absolutely favourable to the freedom of speech, and, on the other hand, the European vision (and other countries), more attentive to the protection of the principles of equality and human dignity, even in the face of the limitation of freedom of expression. Furthermore, it analyses the most relevant jurisprudence cases involving hate speech, with all related most critical issues, regarding the ISP liability and the territorial jurisdiction (because the absence of boundaries on the Internet imposes the need to rethink the boundaries of public law online).

Francesco Di Tano