Ciberspazio e diritto, vol. 16, n. 53 (2-2015), pp. 231-254

GlobaLeaks, piattaforme di whistleblowing e prime applicazioni in Italia

Daniele Bogoni[1]

Sommario: 1. Premessa – 2. GlobaLeaks*:* il framework open source per la gestione dei flussi informativi e la protezione della fonte – 2.1 La procedura di segnalazione – 3. Le iniziative di GlobaLeaks in Italia e nel mondo – 4. Le prime applicazioni di sistemi di whistleblowing in Italia – 5. Conclusioni

1. Premessa

Negli ultimi anni si sono verificati con particolare frequenza casi eclatanti di frodi, fenomeni di corruzione o di altri comportamenti illeciti: tra quelli più celebri si possono citare Enron, WorldCom e, nel nostro Paese, il caso Parmalat.

Per prevenire il ripetersi di casi come questi riveste un ruolo sempre più importante il whistleblowing, strumento legale ideato e presente da tempo negli Stati Uniti d'America e nel Regno Unito per garantire un'informazione tempestiva in merito a eventuali tipologie di rischio attraverso la denuncia di illeciti commessi nei luoghi di lavoro, e non solo[2].

È evidente, infatti, che i primi soggetti in grado di percepire e identificare eventuali irregolarità all'interno di un'impresa, di un ente pubblico o di organizzazioni sono proprio le persone che vi operano e lavorano.

Quando decidono di segnalare tali irregolarità, questi soggetti vengono definiti whistleblower*,* termine inglese che indica «una persona che lavorando all'interno di un'organizzazione, di un'azienda pubblica o privata si trova ad essere testimone di un comportamento irregolare, illegale,

[1] Dottore in Giurisprudenza, laureato in "Informatica Giuridica Avanzata" presso l'Università degli Studi di Milano.

[2] Cfr. C. Florio, "Il whistleblowing nella letteratura internazionale: aspetti definitori e fattori determinanti", «Rivista dei Dottori Commercialisti», fasc. 5, 2007, p. 927.

potenzialmente dannoso per la collettività e decide di segnalarlo all'interno dell'azienda stessa o all'autorità giudiziaria o di portarlo all'attenzione dei media, per porre fine a quel comportamento»[3].

I whistleblowers, infatti, possono svolgere un ruolo fondamentale nell'individuazione di possibili frodi, atti di corruzione e cattiva amministrazione, contribuendo a salvare vite umane, tutelare i diritti umani e garantire il rispetto delle leggi.

Nel fare questo spesso corrono enormi rischi personali: possono subire ritorsioni o persecuzioni sul luogo di lavoro (per esempio mobbing e, nei casi più gravi, provvedimenti di licenziamento), essere citati in giudizio dal datore di lavoro per la violazione del dovere di lealtà e correttezza o per diffamazione e, nei casi estremi, ricevere minacce alla propria incolumità[4].

Recentemente, grazie allo sviluppo di piattaforme tecnologiche per l'invio e la gestione di segnalazioni riguardanti illeciti, reati e episodi di corruzione, è possibile coinvolgere un numero sempre più elevato di persone, che hanno così la possibilità di contribuire alla costruzione di una società più democratica e trasparente.

In questo contesto riveste un ruolo di grande importanza il progetto GlobaLeaks, software che ha permesso di avviare in Italia e in tutto il mondo una serie di iniziative che consentono, nel rispetto dei più elevati standard di sicurezza informatica, lo scambio di informazioni e documenti tra chi decide di segnalare fatti rilevanti e i soggetti riceventi.

Inoltre, anche nella pubblica amministrazione italiana, si assiste a una prima implementazione di piattaforme di whistleblowing che permettono ai dipendenti di segnalare possibili illeciti attraverso una procedura guidata, senza il timore di subire eventuali ritorsioni.

[3] Cfr. M.C. Torchia, "Che cosa indica e come si traduce la parola inglese whistleblower?", 2014, http://www.accademiadellacrusca.it/it/lingua-italiana/consulenza-linguistica/domande-risposte/cosa-indica-come-si-traduce-parola-inglese-w (sito verificato il 22 agosto 2015).

[4] Raccomandazione per una legge sul whistleblowing a cura del Segretariato di Transparency International in Protezione delle "vedette civiche": il ruolo del whistleblowing in Italia, 2009.

Abstract

GlobaLeaks, piattaforme di whistleblowing e prime applicazioni in Italia

Negli anni è cresciuta l'importanza del whistleblowing quale strumento per prevenire il verificarsi di una serie di tipologie di rischio, così come l'esigenza di tutelare chi segnala comportamenti irregolari.
In questo ambito è fondamentale il contributo offerto dalla tecnologia, che ha permesso lo sviluppo di piattaforme di whistleblowing utili per garantire comunicazioni sicure tra chi effettua una segnalazione e chi la riceve.
Tra i progetti più importanti può essere citato GlobaLeaks, software open source che ha consentito a diversi media, aziende pubbliche e private, organizzazioni non governative, di dare vita a diverse iniziative in Italia e in alcune parti del mondo.
Anche nella pubblica amministrazione italiana sono state adottate le prime piattaforme di whistleblowing per tutelare i dipendenti che vogliono segnalare possibili illeciti.

GlobaLeaks, whistleblowing platforms and earlier applications in Italy

Over the years the importance of whistleblowing as an instrument to prevent some risks, as well as the need to protect anyone who reports criminal behaviors, has increased.
In this context it's essential the contribution of some technologies, which have allowed the development of whistleblowing platforms useful to provide safety communications between the whistleblowers and the recipients.
Among the most important projects there is GlobaLeaks, an open source software that has enabled several media, public and private companies, NGO, to begin various initiatives in Italy and in some parts of the world.
Even in the Italian Public Administration was adopted the first whistleblowing platforms to protect employees who want to report possible criminal behaviors.

Daniele Bogoni

Ciberspazio e diritto, vol. 16, n. 53 (2-2015), pp. 255-267

L'odio e la rete: un'introduzione e alcune possibili linee di ricerca

Giovanni Ziccardi[1]

Sommario: 1. L'odio e la rete – 2. Il rapporto tra l'odio circolante e Internet – 3. L'odio e i nuovi toni di discussione – 4. Il necessario approccio interdisciplinare – 5. Le espressioni d'odio

1. L'odio e la rete

Nel momento in cui lo studioso si accinge ad affrontare, e analizzare in dettaglio, il grande tema dell'odio[2], con precipuo riferimento alle espressioni estreme circolanti in Internet e alle nuove forme digitali d'interazione, di dialogo sincrono e asincrono sul web e in chat, di discussione e di attacco tra esseri umani, è facile che il dibattito che si può generare da un simile approfondimento imbocchi molteplici direzioni interpretative, spesso eterogenee tra loro.

In primis, assume importanza centrale un'idea di odio strettamente connessa alle modalità *espressive*, ossia a ciò che in generale, e in senso lato, è comunemente definito *speech* ma che, come è noto, non comprende soltanto il "parlato"[3].

[1] Professore Avvocato Facoltà di Giurisprudenza, Università degli Studi di Milano.

[2] Intendiamo per "odio", in quest'analisi preliminare e in un'idea molto generica, "un sentimento di forte e persistente avversione, per cui si desidera il male o la rovina altrui" o, più genericamente, "un sentimento di profonda ostilità e antipatia". Vedi la voce "odio" in *Vocabolario Treccani*, <http://www.treccani.it/vocabolario/odio/>. Per un'introduzione al tema dell'odio in genere, vedi M. Recalcati, *Sull'odio*, Bruno Mondadori, Milano 2004. Vedi anche, E. Irenäus, *Amore e odio. Per una storia dei comportamenti elementari*, tr. it. Adelphi, Milano 1996. Sull'idea di odio nel contesto sociale e di fragilità e impotenza dell'essere umano vedi il sempre attuale, e fondamentale, E. Fromm, *Fuga dalla libertà*, tr. it. Mondadori, Milano 1987.

[3] In questo ambito, infatti, *speech* sarà sempre inteso in senso lato: non solo come "the expression of, or the ability to, express thoughts and feelings by articulate sounds",

Simile prospettiva ha alimentato la nobile tradizione costituzionalistica nordamericana dell'*hate speech*[4] e della sua protezione ben prima dell'avvento della rivoluzione digitale, con attente analisi che mirano, sovente, a prevedere quali siano le espressioni d'odio che vanno, comunque, *tutelate* al fine di garantire pluralismo e democrazia[5] nella società.

Il tema delle "espressioni d'odio" ha, al contempo, assunto ben presto grande importanza in Europa, con una prospettiva di analisi, soprattutto giuridica, che in molti vedono *contrapposta* a quella nordamericana[6]: ciò che negli Stati Uniti d'America sarebbe *permesso*, in Europa verrebbe, invece, *vietato*[7], per cui l'azione dei legislatori del Vecchio Continente è sovente inquadrata come un processo di riforma volto a *limitare* le espressioni d'odio[8]. Inoltre, l'arrivo "in ritardo" di Internet rispetto al territorio nordamericano ha fatto sì che anche l'Europa si dovesse ben presto confrontare con tematiche giuridico-tecnologiche che negli Stati Uniti d'America erano già state risolte, seppure in un *humus* giuridico ben differente, anni prima.

Oggi l'attenzione per questi temi, e per le importanti implicazioni anche tecnologiche, attira non soltanto ricercatori d'oltreoceano ma anche studiosi, istituzioni politiche e accademiche dell'Irlanda del Nord,

ma come a "formal address or discourse delivered to an audience". Vedi la voce "speech" in *New Oxford American Dictionary*. Per un'introduzione molto curata al rapporto tra odio e libertà d'espressione vedi R. Abel, *La parola e il rispetto*, tr. it. Giuffrè, Milano 1996.

[4] Da intendersi, in senso molto generico, quale "speech that attacks, threatens, or insults a person or group on the basis of national origin, ethnicity, color, religion, gender, gender identity, sexual orientation, or disability". Vedi <http://dictionary.reference.com/browse/hate+speech>.

[5] Con riferimento alla protezione accordata dal Primo Emendamento alla Costituzione degli Stati Uniti d'America vedi, per un'introduzione, P.J. Breckheimer II, "A haven for hate: the foreign and domestic implications of protecting Internet hate speech under the First Amendment", in «Southern California Law Review», vol. 75:1493, pp. 1493-1528.

[6] Vedi, per un'introduzione a questa "contrapposizione" tra i due sistemi, R. Siska, "Hate speech: a comparison between the European Court of Human Rights and the United States Supreme Court Jurisprudence", in «Regent University Law Review», vol. 25:107, pp. 107-118.

[7] Vedi, a tal proposito, R.A. Kahn, "Why do European ban hate speech? A debate between Karl Loewenstein and Robert Post", in «Hofstra Law Review», vol. 41:545, pp. 545-585.

[8] Vedi, su questo punto, C.D. Van Blarcum, "Internet hate speech: the European framework and the emerging American haven", in 62 «Wash. & Lee Review», 781 (2005), pp. 781-830.

Abstract

L'odio e la rete: un'introduzione e alcune possibili linee di ricerca

Il tema delle espressioni d'odio solleva problemi tecnici, giuridici, politici e sociali. Si tratta infatti di un argomento interdisciplinare che ha assunto nuova luce nell'era tecnologica, grazie alla possibilità, finalmente raggiunta, per tutti coloro che hanno una connessione in rete di poter far circolare il proprio pensiero.
In questo articolo si vogliono semplicemente evidenziare delle possibili linee di ricerca, fornendo anche una bibliografia essenziale, su quelli che a nostro avviso sono i temi che nel prossimo futuro solleveranno ulteriori questioni non sempre facili da risolvere.
Il ruolo di Internet nel condizionare – e aumentare – i toni, la difficoltà di gestione del traffico enorme di dati e di commenti, la differente regolamentazione giuridica tra Europa e Stati Uniti d'America, una necessità di auto-regolamentazione (con i conseguenti problemi applicativi) e i nuovi, e dilaganti, fenomeni di odio interpersonale sono probabilmente le più importanti tra dette questioni.

The hate and the network: an introduction and some possible research lines

The hate speech topic raises technical, legal, political and social issues. It is, in fact, an interdisciplinary topic that has acquired a new light in the technological age, with the ability, finally achieved, for all those who have a network connection to spread their ideas.
This article proposes to highlight possible research lines, providing also an essential bibliography on the issues that in the near future will raise and that are not always easy to resolve.
The Internet's role in conditioning – and increasing – the discussion tones, the difficulty of managing the huge traffic of data and comments, the different legal regulation system between Europe and the United States, a need for self-regulation (with its application problems) and the new, and widespread phenomena, of interpersonal hatred are probably the most important of those questions.

Giovanni Ziccardi

Ciberspazio e diritto, vol. 16, n. 53 (2-2015), pp. 271-294

Servizi di pagamento via Internet: il contesto normativo comunitario e italiano sugli aspetti rilevanti ai fini della sicurezza delle operazioni

Gloria Marcoccio*, Ettore Corsini**

1. Premessa

Il settore dei servizi dei pagamenti effettuati per via informatica/telematica tramite l'utilizzo di computer e terminali mobili presenta anche in Italia caratteristiche di spettacolare crescita, come è evidente dall'esperienza di noi tutti nella vita sociale ed in quella professionale[1]. Allo stes-

* Dottore in Ingegneria Elettronica con master in Information Technology Laws presso l'Università La Sapienza di Roma, Lead Auditor ISO27001 e certificata "Privacy Officer e Consulente della Privacy" con TÜV Italia, coordinatore degli studi 'Legal & Privacy in the Cloud' di CSA Italy, reviewer per gli studi FP-7 della Commissione Europea, consulente senior per primarie società multinazionali nel settore delle telecomunicazioni e difesa.

** Dottore in Giurisprudenza presso l'università Luiss Guido Carli, collaboratore presso lo Studio Legale Calvi Luongo Mejia di Roma, socio CSA Italy.

[1] A puro titolo di esempio: - nel 2014 11 milioni di acquirenti "abituali" hanno comprato su Internet almeno una volta al mese. …oltre 200 milioni di transazio-

so tempo ed inevitabilmente si assiste ad un corrispondente eccezionale incremento dei casi di frodi/attacchi informatici ai sistemi di pagamento: ad esempio già nel lontano 2012 nella SEPA[2] ammontava a 794 milioni di euro la stima delle perdite dovute a frodi[3].

La sicurezza dei dati assume, quindi, una importanza strategica in questo settore ed anche a livello di standard vi è grande attenzione nel derivare regolamentazioni e raccomandazioni specifiche come è il caso del PCI Security Standards Councils con le sue recenti pubblicazioni[4].

È però di tutta evidenza l'importanza degli interventi a livello legislativo nello stabilire regole di sicurezza efficaci, adatte in funzione degli specifici mezzi e strumenti di pagamento, tecnologicamente neutre e tali da non creare squilibri tra operatori del settore in base al contesto normativo (nazionale, comunitario, extraeuropeo) che sono vincolati ad osservare.

Il tema è dunque assai ampio e si presta ad innumerevoli e complesse analisi che a nostro avviso al momento offrono una limitata stabilità considerando le dinamicità del settore e delle regole con le quali si intende normarlo, anche alla luce di importanti fenomeni quali le valute virtuali (un esempio su tutti: il *Bitcoin*) potenzialmente destabilizzanti per l'attuale sistema di governo delle valute e relativi mercati. Per tali motivi questo Articolo, parte integrante di apposite attività di studio condotte dagli autori per CSA Italy[5] ha ristretto l'attenzione al caso dei pagamenti

ni nell'intero 2014… *(dati dalla quarta rilevazione trimestrale di fine gennaio 2015 "Net Retail – Il ruolo del digitale negli acquisti degli italiani", realizzata da Netcomm con il supporto di Human Highway e in partnership con Banzai, Postecom e QVC)*, – "Aumenta l'uso del new digital payment nel 2014: +20% rispetto al 2013 per un controvalore di 18 miliardi di euro" (*www.osservatori.net, Infografica 'Mobile payment non manca più nessuno, 2015).*

[2] Single Euro Payments Area.

[3] Cfr. *European Central Bank - February 2014 "Third Report on Card Fraud".*

[4] Cfr. ad esempio "Accepting Mobile Payments with a Smartphone or Tablet" (https://www.pcisecuritystandards.org/documents/accepting_mobile_payments_with_a_smartphone_or_tablet.pdf; indirizzo verificato il 15 settembre 2015).

[5] CSA Italy e`una associazione no-profit di diritto italiano costituita nell'ottobre 2011, Capitolo Italiano di Cloud Security Alliance, associazione internazionale che nasce con lo scopo di promuovere l'utilizzo di best practice per la sicurezza del cloud computing, insieme alla formazione e sensibilizzazione nell'utilizzo sicuro di tutte le forme di *computing*.

Abstract

Servizi di pagamento via Internet: il contesto normativo comunitario e italiano sugli aspetti rilevanti ai fini della sicurezza delle operazioni

La forte crescita del settore dei servizi dei pagamenti digitali effettuati tramite l'utilizzo di computer e terminali mobili, in relazione ai derivanti notevoli rischi connessi alla sicurezza delle operazioni richiede un quadro legislativo stabile in grado di definire regole di protezione efficaci, adatte in funzione degli specifici strumenti di pagamento, tecnologicamente neutre e tali da non creare squilibri tra operatori del settore nel contesto nazionale e comunitario.
L'articolo offre un punto di vista sullo scenario normativo con particolare riferimento alla sicurezza nelle operazioni di pagamento, aggiornato ai recenti interventi da parte della European Banking Authority ed a quelli della Autorità Garante per la Protezione dei Dati Personali in Italia, senza dimenticare di fare un cenno al caso delle Valute Virtuali, potenzialmente destabilizzanti per l'attuale sistema di governo delle valute e relativi mercati.

Payment services via Internet: the Community/Italian legislative framework for the aspects relevant to the security of operations

The strong growth of the sector of digital payments services made through the use of computers and mobile devices, regarding the resulting high risks related to the security of operations, requires a stable legislative framework able to define rules for effective protection, appropriate according to the specific means of payment, and technologically neutral to avoid imbalances between operators at national and EU level.
This work offers a perspective on the regulatory scenario with particular reference to security in payment operations, updated to recent initiatives by the European Banking Authority and those of the Italian Data Protection Authority, without forgetting a nod to the Virtual Currencies case, potentially able to destabilize the current system of government of currency and related markets.

Gloria Marcoccio
Ettore Corsini

Ciberspazio e diritto, vol. 16, n. 53 (2-2015), pp. 295-327

La profilazione degli individui connessi a Internet: privacy online e valore economico dei dati personali

Erika Caterina Pallone[1]

Sommario: 1. Introduzione – 2. Dati personali in cambio di servizi: profilazione come valuta per l'accesso alla società della rete – 3. Valore economico dei dati personali – 4. Profilazione e fidelizzazione – 5. Il caso delle Fidelity Cards – 6. Le grandi potenzialità del marketing sul web e la fortuna di Google – 7. Pubblicità comportamentale online – 8. Pubblicità aggressiva e spamming – 9. Le linee guida del Garante per la protezione dei dati personali – 10. Conclusioni

1. Introduzione

La partecipazione collettiva al mondo digitale ha reso tutti esposti a nuovi pericoli per la propria *privacy*, intesa come diritto alla riservatezza ma anche diritto al controllo delle informazioni che ci riguardano.

Un così alto livello tecnologico è ormai in grado di permeare moltissimi aspetti della vita umana e induce l'utente medio, che accede ai servizi forniti dal web, a rilasciare tutta una serie di informazioni sulle proprie attività in rete, sui luoghi visitati, sui libri letti, sui propri interessi, sui propri legami e su altri aspetti molto intimi dell'individuo[2].

Questo rilascio di dati da parte dell'utente avviene, in una considerevole percentuale di casi, in modo incosciente poiché i processi informatici che permettono di far funzionare, per esempio, un sito web o uno *smartphone* non sono di facile comprensione per i "non-addetti ai lavori".

[1] Dottoressa in Giurisprudenza. Perfezionata in "Informatica Giuridica" presso l'Università degli Studi di Milano. Cultrice della materia "informatica giuridica".

[2] Cfr. A. Savin, *Eu Internet Law*, Cheltenham UK 2013, p. 191, «The dynamism of modern digital life requires participation on a level which forces us to voluntarily relinquish information about our activities, the places we visit, the books we read or the people we befriend».

D'altra parte la tendenza delle nuove tecnologie è proprio quella di essere accessibile per il più ampio numero di persone possibili a prescindere dalla loro cultura, e ciò è possibile da una parte con una estrema semplificazione dei dispositivi elettronici, e dall'altra con un offuscamento, dietro ad un'accattivante interfaccia grafica, di ciò che succede (a livello di processi delle attività) durante il loro utilizzo.

Da qui possiamo dire che, sia l'incoscienza circa la possibilità di registrare e immagazzinare i dati sia la superficialità riservata al valore dei dati personali, portano l'utente del web a fornire direttamente, o attraverso i propri comportamenti, moltissimi dati di carattere personale.

In contrapposizione a questa inconsapevolezza o superficialità dell'utente, c'è invece una lucidissima consapevolezza delle aziende, sia appartenenti al settore dell'*information technology* che a settori diversi, di quanto al giorno d'oggi le informazioni e i dati personali costituiscano preziose merci di scambio, e tanto più tali informazioni possano riguardare aspetti intimi della persona, tanto più appaiono remunerative per chi le utilizza e le fa circolare[3].

Questo rilascio massiccio e costante nel ciberspazio[4] di informazioni corrisponde alla valuta per accedere a servizi e contenuti offerti dal web.

In cambio dei contenuti a cui possiamo accedere, click dopo click, vengono conservati e messi in relazione tra loro dati riferibili ad un determinato soggetto che possono rivelare le più sottili sfumature della sua personalità ma soprattutto mirano a cercare di comprendere cosa spinge all'azione l'utente o ancor di più qual è stato il processo mentale che lo ha portato a compiere quell'azione.

Questo procedimento di raccolta di dati personali e comportamentali e il loro successivo trattamento sfociano nella "profilazione", che raggiunge livelli di ancor maggior penetrazione per gli utenti dei c.d. *social media*, siti di *e-commerce*, *social networks*, *blogs*, motori di ricerca e in generale per i fruitori di servizi di telefonia e comunicazione elettronica[5].

[3] Cfr. S. Rodotà, *Tecnologie e diritti*, Bologna 1995, p. 13.

[4] Il termine ciberspazio è stato usato per la prima volta da William Gibson nel suo romanzo *Neuromante* del 1984 per descrivere come veniva percepita una rete di dati da una mente umana direttamente collegata ad essa.

[5] Cfr. R. De Meo, *Autodeterminazione e consenso nella profilazione dei dati personali*, in «Diritto dell'informazione e dell'informatica», 2013, pp. 587-589.

Abstract

La profilazione degli individui connessi ad Internet: privacy online e valore economico dei dati personali

L'articolo ha lo scopo di gettare maggior luce sul fenomeno della profilazione dei dati personali in Internet, partendo ancor prima da una definizione di dato, privacy e trattamento dei dati personali.
Si tratta di una tecnica di trattamento dei dati personali in continua evoluzione, proprio grazie all'enorme sviluppo della rete e delle nuove tecnologie.
Si è cercato di inquadrare il fenomeno della profilazione partendo dalle possibili finalità per cui tale processo viene messo in atto, con particolare attenzione al valore economico prodotto dai profili desunti tramite la profilazione e al loro possibile utilizzo.
Sotto un profilo strettamente giuridico si delineano dei possibili conflitti tra tale tecnica e alcuni dei nostri diritti, tra cui il diritto alla privacy e alla riservatezza e ancor più diritto all'identità, alla libertà di manifestazione del pensiero, al diritto di libertà religiosa e diritto alla libertà politica.
Tale conflitto è dovuto principalmente all'immissione sempre più inconsapevole di dati che ci riguardano in Internet a tal punto che dalla loro aggregazione è possibile ricavare i più intimi dettagli della personalità di un individuo.
Alla luce di quanto esposto, lo stesso Garante per la protezione dei dati personali ha emesso un provvedimento ad hoc che ha lo scopo di regolamentare la profilazione online effettuata dai gestori di siti Internet e dei servizi ad esso connessi.

The profiling of individuals connected to the Internet: online privacy and the economic value of personal data

The article aims to show more light on the phenomenon of personal data profiling on the Internet, starting even before from a definition of data, of privacy and of personal data.
It is a processing technique of personal data constantly changing, thanks to the enormous development of the network and new technologies.
The purpose is to frame the phenomenon of personal data profiling, starting from the possible finality for which this process is put in place, with particular attention to the economic value generated from profiles obtained through the data profiling, and their possible use.
From a legal point of view, there are possible conflicts between this technique and some of our rights, including the right to privacy and confidentiality, and

even more, for example, the right to identity, to freedom of expression, to freedom of religion and to political freedom.
This conflict is mainly due to the placing increasingly unaware of data that affect us on the Internet, to the point that, from the aggregation is possible to obtain the most intimate details on the personality of an individual.
In light of the above, the Authority for the Protection of Personal Data issued an ad hoc measure that aims to regulate the online personal data profiling carried out by operators of Internet sites and related services.

Erika Caterina Pallone

Ciberspazio e diritto, vol. 16, n. 53 (2-2015), pp. 331-356

La sicurezza informatica di Bitcoin

Davide Candiloro[1]

Sommario: 1. Cosa è Bitcoin – 2. Le classi di minacce di sicurezza – 3. La sicurezza delle operazioni con Bitcoin – 4. Minacce per la rete Bitcoin – 5. Conclusioni: il controllo della rete

1. Cosa è Bitcoin

Bitcoin viene comunemente percepito come una moneta elettronica, un mezzo di pagamento online strettamente legato alla rete Internet, utilizzabile per scambiare denaro tra gli utenti o per effettuare acquisti, mediante transazioni che trasferiscono un valore economico da un soggetto ad un altro, teoricamente in maniera completamente sicura.

Più precisamente, una prima definizione[2] caratterizza *Bitcoin*[3] come un «insieme di concetti e tecnologie che concorre a formare la base di un sistema di moneta digitale. L'insieme dei concetti include una valuta, le cui unità, chiamate *bitcoin,* sono utilizzate per immagazzinare e trasmettere valore tra i partecipanti alla rete *Bitcoin*».

Diverse tecnologie, tra cui quelle crittografiche, supportano il sistema, che nel suo complesso è costituito da programmi software, basati su un algoritmo *open-source*, agenti su una rete informatica detta rete Bitcoin, di dimensione planetaria.

[1] Dottore, Ingegnere laureato presso Politecnico di Milano.

[2] A.M. Antonopoulos, *Mastering Bitcoin*, o'Reilly, 2014, *early preview edition*.

[3] È convenzione diffusa indicare con l'iniziale maiuscola la rete, l'insieme di algoritmi e in generale il sistema Bitcoin. Viceversa si utilizza *bitcoin* con l'iniziale minuscola per riferirsi alle unità di valuta, anche abbreviate con BTC.

La definizione data con il titolo dell'articolo di Satoshi Nakamoto[4], che ha introdotto *bitcoin*, è "*Bitcoin: A Peer-to-Peer Electronic Cash System*", ossia un sistema di denaro elettronico, basato su una rete *Peer-to-Peer*.

Denaro elettronico è da intendersi un sistema di denaro adatto allo scambio e ai pagamenti su Internet, prescindendo dal requisito della compresenza fisica dei soggetti e permettendo di realizzare transazioni istantanee. *Peer-to-Peer* è invece un concetto della teoria delle reti informatiche che caratterizza una rete di calcolatori in cui totalità delle funzionalità richieste alla rete è distribuita tra i singoli nodi, in maniera omogenea e paritaria, senza ricorso ad infrastrutture centrali, in modo che i singoli nodi concorrono alla realizzazione di tutte le funzioni della rete.

Un analogo esempio di questa tecnologia è costituito da diverse reti di *file sharing*[5], dove l'esigenza di operare prescindendo server centrali è emersa in seguito ad azioni legali o attacchi informatici che hanno comportato la chiusura di tali infrastrutture.

Le implicazioni di questo approccio sono molteplici per la rete Bitcoin, che costituisce il primo esempio di rete *Peer-to-Peer* utilizzata per scambiare denaro.

Essa risulta immune a potenziali istanze di chiusura poiché non esiste nessun soggetto da perseguire o da attaccare; dal punto di vista tecnico la disponibilità della rete si svincola dalla disponibilità di strutture centralizzate, e, di contro, gli attacchi informatici delle reti distribuite risultano applicabili anche all'infrastruttura distribuita di Bitcoin.

L'operazione fondamentale distribuita dal protocollo Bitcoin sulla rete decentralizzata è la validazione della sequenza di tutte le transazioni avvenute sulla rete, in modo che ciascun nodo sia in grado di verificare la continuità dei trasferimenti; questa validazione avviene senza la necessità di una terza parte fidata, ed in modo che un potenziale contraffattore della catena delle transazioni debba fornire una prova del lavoro svol-

[4] S. Nakamoto, *Bitcoin: a peer to peer electronic cash system*, 2008. Si tratta dell'articolo che ha introdotto il sistema *Bitcoin*. Il nome Satoshi Nakamoto è uno pseudonimo in quanto il/gli ideatore/i di *Bitcoin* hanno scelto l'anonimato.

[5] Uno degli esempi più rappresentativi è oggi la rete *bittorrent*. Si veda Pouwelse, Johan, et al. "*The bittorrent p2p file-sharing system: Measurements and analysis.*" *Peer-to-Peer Systems IV*. Springer Berlin Heidelberg, 2005. 205-216.

Abstract

La sicurezza informatica di Bitcoin

Bitcoin è stato il primo metodo di pagamento decentralizzato, reso possibile grazie alle odierne tecniche di crittografia combinate in un complesso e innovativo programma che riesce ad evitare in modo sicuro i tipici problemi di una moneta elettronica, come la doppia spesa o la spesa senza titolo. La sicurezza informatica è di estrema importanza per un metodo di pagamento, e ancora di più per un sistema relativamente nuovo come la rete Bitcoin. Se da un lato è possibile riscontrare che minacce convenzionali e già conosciute sono applicabili ai sistemi che costituiscono la rete, nuove classi di minacce sono possibili per via delle peculiarità di Bitcoin. Il presente articolo illustra tutte queste tipologie di vulnerabilità, con riferimento ad un soggetto che mantiene un portafogli per inviare e ricevere pagamenti, a un fornitore di servizi sulla rete, e infine ai problemi che interessano la rete nel suo complesso, giungendo all'analisi del suo controllo.

Computer security of Bitcoin

Bitcoin is the first decentralized payment method, made possible thanks to modern encryption techniques combined into a complex and innovative program that is able to reliably prevent the typical problems of an electronic currency, such as double spending or spending without entitlement. Computer security is extremely important for a payment method, and even more for a relatively new system as the Bitcoin network. While already known and conventional security threats are applicable to the systems that make up the network, new classes of threats are made possible because of the peculiarities of Bitcoin. This article illustrates all these types of vulnerabilities, with reference to an entity that maintains a wallet to send and receive payments, to a service provider on the network, and finally to the problems affecting the network as a whole, leading to the analysis of its control.

Davide Candiloro

Ciberspazio e diritto, vol. 16, n. 53 (2-2015), pp. 357-384

Il controllo a distanza del lavoratore e le nuove tecnologie

Silvia Martinelli[1]

Sommario: 1. Introduzione – 2. L'interpretazione dell'articolo 4 dello Statuto dei Lavoratori nella giurisprudenza della Corte di Cassazione – 3. Il ruolo del Garante per la Protezione dei Dati Personali – 4. Le iniziative della Commissione Europea in materia di protezione dei dati personali dei lavoratori e la Raccomandazione del 1 aprile 2015 del Consiglio d'Europa – 5. La legge delega per il riordino dei rapporti di lavoro, c.d. Jobs Act 2, e lo schema di decreto legislativo approvato in Giugno – 6. L'analisi alla Camera e al Senato – 7. Il parere del Garante per la protezione dei dati personali – 8. L'approvazione definitiva in Consiglio dei Ministri e le prime reazioni – 9. Il nuovo testo dell'articolo 4 dello Statuto dei Lavoratori – 10. Considerazioni conclusive

1. Introduzione

Primo riferimento in materia di controllo a distanza del lavoratore è l'articolo 4 dello Statuto dei Lavoratori (Legge 20 maggio 1970, n. 300), il quale vieta «l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori».

Il Legislatore del 1970, nel regolare l'utilizzo in ambito lavorativo degli strumenti, allora esistenti, in grado di effettuare un controllo a distanza (essenzialmente gli strumenti di videosorveglianza e per il controllo del traffico telefonico), scelse di stabilire, quale regola generale, il divieto al loro utilizzo.

Impianti e apparecchiature dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono, tuttavia, essere installati, ai sensi del secondo comma dell'articolo 4 dello Statuto, se «richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del

[1] Dottoressa in Giurisprudenza. Perfezionata in "Informatica Giuridica", cultrice della materia "Informatica Giuridica" presso l'Università degli Studi di Milano.

lavoro» solo previo accordo con le rappresentanze sindacali aziendali o, in assenza di accordo, mediante il coinvolgimento dell'Ispettorato del lavoro, il quale detta le modalità d'uso degli impianti e le cui determinazioni sono impugnabili entro trenta giorni innanzi al Ministro per il lavoro e la previdenza sociale.

La regola stabilita dall'articolo 4 è, quindi, il divieto di utilizzo, superabile solo ove vi siano particolari esigenze – organizzative, produttive o connesse alla sicurezza del lavoro – ed esclusivamente al fine di soddisfare tali esigenze.

La norma, collocata nel Titolo I dello Statuto dei Lavoratori, mira alla tutela della dignità del lavoratore, assicurando che il controllo sull'attività lavorativa sia operato direttamente da persone fisiche, anziché mediante l'utilizzo di apparecchiature. Tale seconda tipologia di controllo presenta, infatti, una maggiore invasività, in quanto, potendo assumere le forme del controllo continuativo, anelastico o occulto, tende a ledere la zona di riservatezza e autonomia del dipendente nello svolgimento della prestazione lavorativa e a sottoporlo a una forte pressione psicologica[2].

Nonostante la datazione della norma, il Legislatore ha colto tale problematica, proteggendo il lavoratore da forme di controllo idonee a essere così invasive da porre in pericolo la riservatezza e la dignità del lavoratore.

Tale scelta, seppur lungimirante, è stata adottata in un contesto nel quale gli strumenti idonei ad effettuare tale tipologia di controllo erano piuttosto esigui, se rapportati a quanti ve ne sono nel mondo odierno, e certamente meno invasivi e pervasivi.

Nell'ultimo ventennio, l'utilizzo dell'informatica – dal computer alla posta elettronica, dalla navigazione in Internet ai Social Network – è divenuto essenziale nella maggior parte delle attività lavorative. Sono strumenti quotidianamente utilizzati, tutti in grado di memorizzare ogni azione compiuta dal lavoratore.

Tali mutamenti, in assenza di un intervento legislativo, hanno imposto una riflessione interpretativo-evolutiva della norma statutaria, intervenuta ad opera della giurisprudenza e del Garante per la Protezione dei Dati Personali.

[2] Cfr. I. Alvino, "L'articolo 4 dello Statuto dei lavoratori alla prova di Internet e della posta elettronica", in «Diritto delle Relazioni Industriali», fasc. 4, Giuffré 2014, p. 999.

Abstract

Il controllo a distanza del lavoratore e le nuove tecnologie

L'articolo 4 dello Statuto dei lavoratori, primo riferimento in materia di controllo a distanza dei lavoratori, è stato recentemente modificato con D.lgs. n. 151 del 14 settembre 2015, in attuazione della legge delega per il riordino dei rapporti di lavoro, c.d. Jobs Act 2. L'articolo descrive la disciplina del controllo a distanza del lavoratore mediante le nuove tecnologie prima di novella, secondo le interpretazioni fornite dalla Suprema Corte e dal Garante per la protezione dei dati personali, e ripercorre il processo legislativo che ha portato alla modifica (con particolare attenzione all'analisi svolta presso le Camere ed alle osservazioni del Garante per la protezione dei dati personali), per giungere all'analisi del testo novellato nell'ottica di un confronto con la disciplina previgente.

The remote control of the employee and the new technologies

Article 4 of "Statuto dei lavoratori", the most important Italian labor law, was recently amended by Decree. n. 151 of 14 September 2015, in accordance with law for the reorganization of labor relations ("Jobs Act 2").
The essay delineates the rules applicable to remote control of the employee before the amendment, according to the interpretations provided by the Supreme Court and the Data Protection Authority. Afterwards it describes the legislative process, especially with regard to the Parliament's analysis and the opinion of the Data Protection Authority. Finally it analyze the new text of article 4, in comparison with the previous legislation.

Silvia Martinelli