Ciberspazio e diritto, vol. 15, n. 50 (1-2014), pp. 11-26

"Fourth generation" payment systems: Bitcoins

Valentina Amenta[1]

Index: 1. Introduction: historico-juridical organization. – 2. The Bitcoin: its creation. – 3. Legislation regarding Bitcoins. – 3.1. The jurisdiction of Bitcoins in United States regulations. – 3.2. The jurisdiction of Bitcoins in European regulations. – 3.3. Bitcoin jurisdiction in Italian regulations. – 4. Conclusions.

1. Introduction: historico-juridical organization

In the last two decades payment systems[2] have evolved rapidly, due to the increasingly complex range of production processes as well as the exponential growth of the many payment services offered by customers.

The increased use of innovative technologies, along with the positive attitude of the system's operators, has contributed to the passage from the real concept of currency, understood as *traditio* of pieces of money, to the mandatory concept of payment, in which the transfer of sums of money, freed from material delivery, is carried out through the transmission of electronic impulses that are a direct expression of the monetary position.

The most evolved form of this means of payment, effectively defined by some as "fourth generation" (Sword, 1976) payment systems, after the era of legal currency, deposit currency and bank money, involves electronic money and crypto-currency.

E-money, electronic money, e-purse and digital currency are several expressions now in the common parlance; their unstoppable affirmation

[1] Valentina Amenta, CNR Institute of Informatics and Telematics, Pisa, Italy.

[2] A payment system is the complex and subdivided infrastructure that in modern economies supports the functionality and efficiency of trade in goods, services and financial assets. It can be defined as a complex institutional apparatus of standards, controls, intermediary producers of monetary genres and of financial services that support the transfer of money to fulfill the obligations assumed by economic operators when they acquire the rights to real and financial resources.

in the current socio-economic situation made inevitable the intervention of the European Community lawmaker who enacted comprehensive legislation divided into three directives: n. 200/28/CE and n. 2000/46/EC, both issued September 18, 2000 concerning the launch, practice and precautionary supervision of the activities of institutes issuing electronic money, and finally, Directive no. 2009/110/EC, published on October 10, 2009 amending Directives 2005/60/EC and 2006/48/EC and repealing the abovementioned Directive 2000/46/EC.

As a legacy of that Directive, the definition of electronic money[3] is now repealed in which it is defined as "monetary value represented by a claim on the issuer that is stored on an electronic device, issued on receipt of funds, the value of which is not less than the monetary value issued and accepted as a means of payment for enterprises other than that of the issuer".

Therefore, based on this definition it is necessary to identify the defining characteristics of the case, starting with the term "monetary value".

In a published Opinion concerning the proposal for a directive, the European Central Bank expressed some reservations on whether to include this phrase in the definition of electronic money, considering it too generic and indicating instead "redeemable claim" as a more coherent expression). In fact, the Community legislator has only partially accepted the proposals made by the European Central Bank. In fact, he has preferred to retain the qualification of electronic money in terms of "monetary value". Directive n. 2009/11/EC takes it a step further; in fact, the reference to "electronic device" is deleted in the definition of electronic money, in such a way as to also cover in this case merely virtual media (such as the hard disk of one's own computer), which thus paves the way to crypto-currency/money.

[3] In Italy, the use of electronic money is increasingly widespread, although the gap between Italy and the rest of Europe remains significant. This is due to the psychological resistance to new technologies that has always characterized our country. Recent studies (Assofin-CRIF Decision Solutions-GfK Eurisko, related to the 2012 final balance) reveal the presence of 71.2 million payment cards in Italy, on average 1.2 per inhabitant. The number has increased considerably in the last five years, but remains lower than the EU average (1.5), not to mention that of more virtuous countries such as the UK (2.4 per capita) and Sweden (2.2)

Abstract

"Fourth generation" payment systems: Bitcoins

The globalization of markets, with the introduction of a single currency and the elimination of borders in providing services, has led to significant consequences in a number of areas; among these a prominent place is occupied by the payment industry. We are witnessing the passage from the real concept of currency, seen as a traditio of monetary prices, to the mandatory concept of payment, in which the transfer of sums of money, freed from material delivery, occurs through the transmission of electronic pulses that are a direct expression of the monetary position. The most evolved form of this means of payment, effectively referred to by some as "fourth generation" payment systems, after the era of legal currency, deposit currency and bank money, is electronic money, otherwise known as e-money. Thus, the Article will focus on a new development in electronic money, the Bitcoin. It is a decentralized virtual currency that is not controlled by any bank or financial intermediary, and is coined at home via one's own computer. The success of this currency has resulted in an intrinsic increase in its price, so from a mere means of transaction it has become a safe-haven asset for many people.

I sistemi di pagamento di "Quarta generazione": Bitcoins

I sistemi di pagamento in tutto il mondo stanno osservando con attenzione la diffusione del sistema Bitcoin, un sistema di pagamento strettamente connesso alla rete e a una nuova idea di trasferimento di denaro. Definito come un sistema di pagamento di "quarta generazione", l'e-money solleva problemi giuridici di grande interesse per lo studioso, sia per la sua decentralizzazione e il suo aspetto personal (correlate al singolo computer dell'utilizzatore) sia per la mancanza di un vero e proprio controllo da parte di banche o intermediary finanziari. L'Articolo illustra la natura di questo sistema di pagamento e il rapport con la giurisdizione di diversi Paesi.

Valentina Amenta

Ciberspazio e diritto, vol. 15, n. 50 (1-2014), pp. 27-36

Le nuove modalità di ricerca nelle banche di dati giuridiche: alcune considerazioni (e un'ipotesi di ricerca)

Giovanni Ziccardi

Indice: 1. Legal Information Retrieval e informatica giuridica. – 2. Un tema suggestivo (e "circolare"). – 3. Una proposta di ricerca.

1. Legal Information Retrieval *e informatica giuridica*

L'individuazione di fonti e informazioni normative, giurisprudenziali, dottrinali e bibliografiche per alimentare un archivio elettronico, il reperimento dei testi integrali dei provvedimenti, la redazione di abstract o la massimazione di sentenze, la raccolta sistematica – e la più esaustiva possibile – dei dati, la marcatura[1], la catalogazione, la pubblicazione offline e online e la successiva attività di ricerca automatizzata dei testi all'interno della grande banca di dati così costituita sono, tutti, aspetti peculiari di quel settore di studio dell'informatica giuridica definito *Legal Information Retrieval* (d'ora

[1] Per *marcatura*, in tale contesto informatico-giuridico, s'intende l'etichettatura tramite codici informatici di alcuni termini (o di parti/porzioni di testo) affinché possano essere riconosciute da un sistema elettronico che, in un secondo momento, le andrà a elaborare. Per un'introduzione al tema della "marcatura" di documenti giuridici si vedano: M.P. Giovannini, M. Palmirani, E. Francesconi, *Linee guida per la marcatura dei documenti normativi secondo gli standard NormeInRete*, Firenze, European Press Academic Publishing 2012; M. Palmirani, *Legislative XML: Principles and technical tools*, Roma, Aracne 2012 M. Palmirani, G. Governatori, A. Rotolo, S. Tabet, H. Boley, A. Paschke, *LegalRuleML: XML-Based Rules and Norms*, in M. Palmirani, D. Sottara (a cura di), *Rule-Based Modeling and Computing on the Semantic Web*, Heidelberg, Spinger 2011; G. Sartor, M. Palmirani, E. Francesconi, M.A. Biasiotti (a cura di), *Legislative XML for the Semantic Web*, Heidelberg, Springer 2011.

in avanti: LIR)[2] che interessa gli studiosi della materia da oltre settant'anni[3].

In questi anni si stanno manifestando alcuni cambiamenti degni di nota che assumono, per lo studioso del diritto, un particolare rilievo, soprattutto nell'ambito delle modalità con cui è (e sarà) effettuata la *ricerca* di informazioni all'interno di sistemi diventati sempre più complessi.

I mutamenti repentini in tali ambiti, è ben noto, sono inevitabili.

I progetti di LIR si sono sempre adeguati all'incessante evoluzione tecnologica, che ha assunto connotazioni "rivoluzionarie" negli ultimi

[2] Già nel 1969 lo studioso israeliano Aviezri S. Fraenkel, nel suo saggio intitolato *Legal Information Retrieval* (cfr. A.S. Fraenkel, *Legal Information Retrieval*, in F.L. Alt, M. Rubinoff (a cura di), *Advances in Computers*, Vol. 9, San Diego, Elsevier, pp. 113-178), notava come sarebbe più rigoroso, in realtà, utilizzare l'espressione *Legal Document Retrieval* (p. 115), più legata al concetto di *documento*. Si vedano anche, per una prima introduzione all'argomento, K. Tamsin Maxwell, B. Schafer, *Concept and Context in Legal Information Retrieval*, all'indirizzo http://homepages.inf.ed.ac.uk/s0676227/MaxSchaf_legalIR_NLPvKE.pdf; C.D. Hafner, *Representation of Knowledge in a Legal Information Retrieval System*, all'indirizzo http://www.egov.ufsc.br/portal/sites/default/files/anexos/5714-5706-1-PB.pdf; J. Saias, P. Quaresma, *Semantic Enrichment of a Web Legal Information Retrieval System*, all'indirizzo http://www.jurix.nl/pdf/j02-02.pdf (siti web consultati, e documenti disponibili online, l'8 marzo 2014).

[3] In tutti i Paesi, compresa l'Italia, l'interesse scientifico per la ricerca automatizzata di informazioni giuridiche coincise con la diffusione dei primi, potenti calcolatori che erano in grado di organizzare enormi quantitativi di dati, inizialmente appannaggio esclusivo di istituzioni pubbliche o grandi realtà private. Tale evoluzione storica è ricordata in quasi tutti i testi più recenti di informatica giuridica. Si vedano, *inter alia*: M. Jori (a cura di), *Elementi di informatica giuridica*, Torino, Giappichelli 2006; G. Sartor, *L'informatica giuridica e le tecnologie dell'informazione*, Torino, Giappichelli 2012; G. Ziccardi, *Informatica giuridica* (Tomo I), Milano, Giuffrè 2011; G. Taddei Elmi, *Corso di informatica giuridica*, Napoli, Edizioni Giuridiche Simone 2010; M. Durante, U. Pagallo (a cura di), *Manuale di informatica giuridica e di diritto delle nuove tecnologie*, Torino, UTET 2012; E. Florindi (a cura di), *Computer e diritto. L'informatica giuridica nella società dell'informazione e della conoscenza*, Milano, Giuffrè 2012. Circa, invece, i primi pionieri della materia e gli approcci teorici originari (nonché quelli più moderni) al tema si vedano, *inter alia*: F. Romeo, *Lezioni di logica e informatica giuridica*, Torino, Giappichelli 2012; M.G. Losano, *Corso di Informatica Giuridica*, Torino, Einaudi 1986; R. Borruso, S. Russo, C. Tiberi, *L'informatica per il giurista. Dal Bit a Internet*, Milano, Giuffrè 2009; R. Borruso, *Computer e diritto*, Milano, Giuffrè 1988; Id., *Civiltà del computer*, Milano, IPSOA 1978; L. Floridi, *Infosfera. Etica e filosofia nell'età dell'informazione*, Torino, Giappichelli 2009; Id., *La rivoluzione dell'informazione*, Torino, Codice 2012; M. Durante, *Il futuro del web. Etica, diritto, decentramento. Dalla sussidiarietà digitale all'economia dell'informazione in rete*, Torino, Giappichelli 2007.

Abstract

Le nuove modalità di ricerca nelle banche di dati giuridiche: alcune considerazioni (e un'ipotesi di ricerca)

The issue of legal databases and Legal Information Retrieval, and of the search activity in a large volume of documents, has always been particularly fascinating to the scholar of legal informatics. In recent years, in addition to traditional problems, lines of research have been developed concerning advanced searching for documents, with particular regard to the possibility of providing the user questions (and their needs) and present (ranking) results in a way that is as close as possible to the content desired. In this Article the author outlines some points which, in his opinion, may raise very innovative and interesting issues.

Le nuove modalità di ricerca nelle banche di dati giuridiche: alcune considerazioni (e un'ipotesi di ricerca)

Il tema delle banche di dati giuridiche, e della ricerca all'interno di una grande mole di documenti, è sempre stato particolarmente affascinante per lo studioso di informatica giuridica. Negli ultimi anni, accanto a problematiche tradizionali, si sono sviluppate linee di ricerca molto attente alla fase di ricerca dei documenti, con particolare riguardo alla possibilità di prevedere le domande dell'utente (e le sue esigenze) e di presentare (ranking) i risultati in una modalità che sia la più vicina possibile ai suoi desiderata. In questo Articolo si delineano alcuni punti che, a parere dell'Autore, possono sollevare questioni molto innovative e interessanti.

Giovanni Ziccardi

Ciberspazio e diritto, vol. 15, n. 50 (1-2014), pp. 39-70

Trasparenza, apertura e controllo democratico dell'amministrazione pubblica

Fernanda Faini[1]

Indice: 1. L'amministrazione digitale e l'*open government*. – 2. L'evoluzione normativa del principio di trasparenza. – 3. Il d.lgs. 33/2013: il diritto alla conoscibilità e il riordino della disciplina in materia di trasparenza. – 4. Il paradigma dell'apertura: gli *open data* nel quadro normativo attuale. – 5. Il controllo democratico nelle recenti norme in materia di trasparenza e apertura.

*1. L'amministrazione digitale e l'*open government

L'evoluzione della realtà grazie all'ingresso e all'impatto pervasivo delle tecnologie dell'informazione e della comunicazione su ogni aspetto della vita individuale e sociale ha comportato l'utilizzo del termine "società dell'informazione e della conoscenza" per definire l'assetto delle società industriali avanzate, basato sulla centralità dell'informazione e della conoscenza quali risorse essenziali per lo sviluppo economico, sociale e culturale[2]. Il termine "società dell'informazione" in Europa compare fin dal 1993 nel c.d. Rapporto Delors (Libro bianco su Crescita, Compe-

[1] L'Autrice è laureata in Giurisprudenza presso l'Università degli Studi di Firenze e ha conseguito il Master universitario di secondo livello in Management pubblico ed E-government presso l'Università del Salento. 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 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 "Il Documento Digitale". Autrice di pubblicazioni scientifiche e relatrice in convegni, seminari e conferenze in materia.

[2] In tal senso la definizione di società dell'informazione e della conoscenza di cui all'art. 3, lett. b), della legge regionale toscana 26 gennaio 2004, n. 1, recante *Promozione dell'amministrazione elettronica e della società dell'informazione e della conoscenza nel sistema regionale. Disciplina della "Rete telematica regionale toscana"*.

titività, Occupazione): l'informazione è vista come ricchezza ed elemento chiave dei processi economici e sociali per lo sviluppo dei mercati e la crescita europea.

Già dal termine che la connota emerge quale caratteristica determinante della società odierna la centralità dell'informazione che diventa il principale bene economico, "la materia prima" delle nuove tecnologie[3]. Le nuove tecnologie consentono una crescita enorme delle informazioni disponibili e permettono di avvalersi di strumenti automatici per acquisirle, generando una forte riduzione dei costi di raccolta e connotando la società per nuove modalità di interconnessione, cooperazione, integrazione. La crescita delle informazioni disponibili e il facile accesso alle stesse per mezzo della tecnologia comportano, di conseguenza, cambiamenti profondi nel modo di avere e di creare la conoscenza[4].

Semplicità e immediatezza sono le *keywords* del web e della nuova società della rete (*network society*): mutano profondamente le relazioni fra gli individui, che diventano semplici e immediate, in quanto vengono abbattuti gli ostacoli della distanza territoriale e temporale[5]. La società contemporanea è caratterizzata dal principio di *openness*, che favorisce un approccio "a rete" in grado di creare sinergie inedite tra i soggetti e di generare idee, soluzioni inesplorate, nuovi servizi e prodotti: il concetto di conoscenza viene valorizzato come bene comune ed emerge l'intelligenza collettiva[6].

[3] In tal senso e, più ampiamente, sulla società dell'informazione cfr. M. Castells, *The rise of the Network society*, Oxford, Oxford University Press 2000.

[4] Nella società contemporanea si pongono nuove problematiche e nuove esigenze di sicurezza non solo dei sistemi, delle infrastrutture e del loro funzionamento, ma anche dei dati e delle informazioni, così come dei soggetti, che non devono perdere il controllo della propria rappresentazione informatica (diritto all'autodeterminazione sulle proprie informazioni) e devono essere protetti da reati e frodi informatiche.

[5] Nella società dell'informazione, la "virtualità" comporta cambiamenti nel fattore "tempo", dal momento che le tecnologie rendono sostanzialmente immediata la trasmissione delle comunicazioni. Inoltre si modifica il fattore "spazio", in quanto la cosiddetta società della rete si caratterizza per l'aterritorialità: le tecnologie permettono di prescindere dal vincolo territoriale e dalle distanze geografiche. Cfr. G. Sartor, *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, seconda edizione, Torino, Giappichelli 2010, p. 1 e ss.

[6] Secondo P. Lévy, *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, trad. it., Milano, Feltrinelli 1996, p. 34 e ss. l'intelligenza collettiva è «un'intelligenza

Abstract

Trasparenza, apertura e controllo democratico dell'amministrazione pubblica

Lo sviluppo della società contemporanea ha comportato l'evoluzione dell'amministrazione pubblica verso il modello di *open government* caratterizzato dai principi di trasparenza, partecipazione e collaborazione.
In particolare il principio di trasparenza ha conosciuto un crescente interesse nei suoi confronti da parte della normativa, particolarmente accentuato negli ultimi anni e culminato nel d.lgs. 33/2013. Il decreto legislativo amplia, rafforza e struttura il principio di trasparenza che viene reso maggiormente effettivo con l'accesso civico, con strumenti di vigilanza e specifiche sanzioni.
La trasparenza matura anche nella sua natura, dal momento che le disposizioni normative hanno posto attenzione crescente non solo alla quantità dei dati che devono essere pubblicati (al *quantum*), ma anche al "come" dei dati, al *quomodo* della trasparenza, al suo aspetto dinamico e attivo, agli *open data.*
Pertanto nelle disposizioni trasparenza e apertura si coniugano, al fine di realizzare i principi costituzionali dell'agire pubblico e permettere il controllo democratico sull'azione amministrativa.
Il controllo democratico, funzionale al buon andamento dell'amministrazione pubblica, viene rafforzato dall'*openness* e dalla possibilità di riutilizzo dei dati e viene favorito da un insieme di elementi e strumenti esplicitamente regolati dalle nuove disposizioni.
In conclusione, nello sviluppo che porta le amministrazioni pubbliche ad assumere i tratti distintivi dell'*open government*, l'evoluzione normativa relativa ai principi di trasparenza e apertura consente un controllo democratico più semplice, più effettivo e quindi più efficace, che per trovare concreta attuazione necessita della consapevolezza della collettività e della responsabilizzazione delle amministrazioni pubbliche.

Transparency, openness and democratic control of public administration

The development of contemporary society has led to the evolution of public administration towards the model of open government, which is characterized by the principles of transparency, participation and collaboration.
In particular, legislation has shown a growing interest in the principle of transparency, accentuated in recent years and culminated in the Legislative Decree no. 33/2013. The decree expands, strengthens and structures the principle of

transparency, made more effective by the prevision of "civic access", with tools of surveillance and specific sanctions.
Transparency also evolves in its nature, since the regulations have placed increasing emphasis not only to the quantity of data to be published (the "quantum"), but also to their format (the "quomodo"), which leads to the concept of open data.
Therefore, the provisions for transparency and openness are combined, in order to achieve the constitutional principles of public action and to allow democratic control on administrative action.
Democratic control, which is functional to the good performance of the public administration, is strengthened by the openness and the possibility of re-use of data. It is also favored by a set of elements and instruments expressly governed by the new provisions.
In conclusion, in the process that leads the government to take the hallmarks of open government, regulatory developments on the principles of transparency and openness lead to an easier and more effective democratic control. To find concrete implementation, this requires awareness of the community and accountability of government.

Fernanda Faini

Ciberspazio e diritto, vol. 15, n. 50 (1-2014), pp. 73-95

Social media security: introduzione teorica e possibile approccio

Carlo Bernardi[1], Simone Bonavita[2], Mattia Reggiani[3]

Indice: 1. Introduzione. – 2. Verso una possibile definizione di *social media security* – 3. Aziende e social network. – 4. Rischi associati. – 5. Tipologie d'attacco. – 6. Casi concreti. – 7. Social media e sicurezza. – 8. Un possibile approccio alla *social media security*. – 9. Aspetti contrattuali. – 10. Policy e disposizioni organizzative. – 11. Il software di monitoraggio e sicurezza. – 12. Stato dell'arte delle *API*. – 13. Conclusioni.

1. Introduzione

I social network hanno rappresentato una vera e propria rivoluzione del web all'inizio del ventunesimo secolo. Con il loro avvento il nostro rapporto con la Rete e il nostro stile di vita sono drasticamente cambiati: costantemente connessi, trascorriamo le nostre giornate a sfogliare album fotografici, a leggere impressioni, a commentare, ma soprattutto a condividere le nostre esperienze con il web. Sempre più spesso la vita nel social network appare più interessante di quella reale e lo scopo primo di molti di noi diventa quello di arricchire il proprio profilo, di aggiungere nuovi amici, di rendersi interessanti, di dire sempre dove e con chi ci si trova, di far parte di questa vita.[4] Pur di ottenere consensi e approvazioni si accetta di sacrificare la propria privacy, rinunciando peraltro alla piacevolezza del tenere per sé e fare proprie alcune particolari esperienze. Sono

[1] Dottore in Sicurezza dei Sistemi e delle Reti Informatiche, Università degli Studi di Milano.

[2] Cultore della materia di Informatica Giuridica presso l'Università degli Studi di Milano.

[3] Dottore in Informatica, perfezionato in *Cyber Warfare*, Università degli Studi di Milano.

[4] Per approfondire l'aspetto sociologico dei social network ricordiamo l'opera di D. Bennato, *Sociologia dei media digitali. Relazioni sociali e processi comunicativi del web partecipativo*, Laterza 2011.

sempre più frequenti le situazioni nelle quali le persone che si ritrovano fisicamente, trascorrono l'intero incontro senza staccarsi dal proprio smartphone, scattando foto al cibo che stanno per mangiare e rispondendo alle chat, perdendosi così il piacere dello stare assieme e di vivere quello che li circonda.[5]

D'altra parte le aziende[6], consapevoli di questo fenomeno, stanno rivolgendo sempre maggior attenzione ai social network. Con lo scopo di migliorare il rapporto con i clienti, promuovere le campagne pubblicitarie, fidelizzare i clienti ed aumentare il proprio mercato, esse decidono di avere un loro spazio all'interno dei social network.[7]

È in questo contesto che l'articolo vuole proporre al lettore alcuni punti di riflessione per comprendere ed approfondire il concetto di *social media Security*, un argomento ancora poco discusso e conosciuto nelle aziende e tra i privati, ma che ha già suscitato molta attenzione all'interno degli ambiti di ricerca e che sta divenendo il focus primario dei report specialistici.

Quali sono i problemi e i rischi che nascono utilizzando un social media in ambito aziendale? Si pone attenzione a problemi quali trattamento dei dati sensibili, protezione della privacy, protezione del marchio e della web identity? Esistono delle policy[8] aziendali che regolano la

[5] Per approfondire il fenomeno sociale del distaccamento rimandiamo all'opera di Laura Iannelli, *Facebook & Co. Sociologia dei social network sites*, Guerini Scientifica 2011.

Ricordiamo inoltre la recente campagna pubblicitaria, targata *The Coca-Cola Company*, dal titolo "Coca-Cola social media Guard".

[6] All'interno di questo articolo, si usa il termine *azienda* nell'accezione generale di *organismo economico composto di persone e di beni rivolti al raggiungimento di uno scopo determinato* e non nell'accezione legislativa di *complesso dei beni organizzati dall'imprenditore per l'esercizio dell'impresa*. Entrambe le definizioni sono tratte dal vocabolario di lingua italiana *Treccani*.

[7] Per una approfondita analisi del fenomeno si ricorda l'opera a cura di Bruno Lamborghini, *L'impresa Web. Social Network e Business Collaboration per il rilancio dello sviluppo*, Franco Angeli 2009.

[8] Una *policy*, ovvero un principio, un protocollo per guidare le decisioni e ottenere risultati razionali. Una policy è quindi una dichiarazione di intenti, ed è implementata attraverso una procedura od un protocollo. Ricordiamo, a tal proposito, l'opera di T.R. Peltier, *Information Security Policies, Procedures, and Standards*, Auerbach 2001.

Abstract

Social media security: theoretical introduction and a possible approach

The arrival and recent diffusion of social networks in the business environment raised new issues regarding information Security and Privacy. In this paper the main risks related to these issues are analyzed and the new concept of *social media Security* is introduced. Thereafter, the authors describe an approach that merges contractual aspects with a policy and a security software, in order to mitigate the most common adverse events.

Social media security: introduzione teorica e possibile approccio

L'avvento dei social network e la loro recente diffusione in ambito aziendale hanno fatto emergere nuove problematiche di sicurezza informatica e di tutela della privacy. Con questo articolo vengono analizzati i principali rischi associati a queste problematiche e si introduce il concetto di *social media security*. Gli autori descrivono successivamente un approccio che fonde aspetti contrattuali ad una policy e ad un software di sicurezza, allo scopo di mitigare gli eventi avversi più comuni.

Carlo Bernardi
Simone Bonavita
Mattia Reggiani

Ciberspazio e diritto, vol. 15, n. 50 (1-2014), pp. 99-143

L'informatica forense e i modelli di investigazione digitale

Antonio Fiore[1]

Indice: 1. Introduzione. – 2. L'informatica forense. – 3. I primi modelli di investigazione. – 4. Dall'*Integrated Digital Investigation Process Model* alla sua evoluzione: l'*Enhanced Digital Investigation Process Model*. – 5. Dall'*Extended Model of Cybercrime Investigation* al *Dual Data Analysis Process*. – 6. I recenti modelli di *Digital Forensic Investigation*. – 7. Conclusioni.

1. Introduzione

La diffusione e l'utilizzo delle nuove tecnologie dell'informazione e della comunicazione ha cambiato radicalmente il modo di vivere, lavorare, comunicare e apprendere, ma nel contempo ha favorito il manifestarsi di nuove fattispecie di reato legate all'utilizzo di sistemi informatici e telematici[2], ha "traslato" alcuni reati non informatici nel mondo virtuale e ha inoltre favorito fattispecie criminali che non rientrano nell'ambito dei reati informatici in senso stretto, ma sono legate all'utilizzo dei dispositivi digitali divenuti di fatto fonti di informazioni dai quali trarre elementi di prova o indizi utili ai fini delle indagini dal punto di vista fisico/biologico (es. impronte digitali, analisi del DNA) ma soprattutto logico (es. dati e/o informazioni).

Tutte le operazioni effettuate da un utente su un sistema di elaborazione informatico e/o telematico lasciano delle tracce che possono costituire prove di un'attività illecita, le cosiddette prove o evidenze digitali (*digital evidence*), ossia le prove legali ottenute attraverso sistemi digitali. La prova digitale è qualsiasi informazione con valore probatorio creata,

1 Dottore in Giurisprudenza e in Scienze Politiche. Ha conseguito il Master in Public Management, il Master in Tecnologie e Gestione del Software e la certificazione informatica EUCIP IT Administrator. È docente di discipline giuridiche ed economiche, giornalista pubblicista e sistemista informatico.

2 I cosiddetti reati informatici in senso stretto introdotti dalla Legge 23 dicembre 1993 n. 547, recante "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

trasmessa o memorizzata in forma binaria attraverso dispositivi elettronici[3] e al fine di recuperare ed analizzare tali informazioni si ricorre all'informatica forense.

[3] La letteratura scientifica ha dato diverse definizioni di "*digital evidence*". Cfr. Scientific Working Group On Digital Evidence, International Organization On Digital Evidence, *Digital Evidence: Standards and Principles*, «Forensic Science Communications», vol. 2, n. 2, April 2000, in http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm (04-02-2014) ha definito: «Digital evidence is any information of probative value that is either stored or transmitted in a binary form.» Per E. Casey, *Digital Evidence and Computer Crime*, London, Academic Press 2000: «any data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator.»; per J.W. Chisum, *Crime Reconstruction and Evidence Dynamics*, presented at the Academy of Behavioral Profiling Annual Meeting, Monterey, CA., 1999; riproposto in E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (second edition) Elsevier Academic Press CA 2004, p. 12 e in E. Casey, Digital *Evidence and Computer Crime: Forensic Science, Computers and the Internet*, (third edition) Elsevier 2011, p. 7: «any data stored or transmitted using a computer that support or refuse a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi». B. Carrier, *A hypothesis-based approach to digital forensic investigations* (PhD thesis), Purdue University 2006, p. 11 si riferisce a «digital data that supports or refutes a hypothesis about digital events or the state of digital data». Secondo la definizione dell'International Organization on Computer Evidence (IOCE), 2000: «Electronic evidence is information generated, stored or transmitted using electronic devices that may be relied upon in court». The Association of Chief Police Officers (ACPO), *Good Practice Guide for Computer Based Electronic Evidence*, 7Safe, 2000, p. 4 definisce «Computer-based electronic evidence is information and data of investigative value that are stored on or transmitted by a computer» e per M.B. Mukasey, J.L. Sedgwick, D.W. Hagy (National Institute of Justice), *Electronic Crime Scene Investigation: A Guide for First Responders*, April 2008, p. IX: «Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an eletronic device». Per G. Shrivastava, K. Sharma, A. Dwivedi, *Forensic Computing Models: technical overview*, «Computer Science & Information Technology» (CS & IT), vol. 2, n. 2, 2012, p. 209: «Digital evidence is defined as the clues which can be recovered from digital sources…». Per S. Mason, "Sources of Digital Evidence" in S. Mason, *Electronic Evidence: Disclosure, Discovery and Admissibility*, London, Lexis Nexis Butterworths 2007, par. 2.01: «Examples of evidence obtained from analogue devices include vinyl records, audio tape, photographic film and telephone calls made of the public switched telephone network. Analogue systems or products generate evidence in the form of data that is capable of being produced in a permanent form. […] Examples of digital data include anything that has been created or stored on a computer or is made available by way of the Internet, including Cds, DVDs, MP3s and digital broadcast radio». Inoltre, S. Mason, op. cit., par. 2.03, aggiunge: «Electronic evidence: data (comprising the output of analogue devices or data in digital format) that is created, manipulated, stored or

Abstract

L'informatica forense e i modelli di investigazione digitale

L'informatica forense è una branca della scienza forense che si occupa di identificare, acquisire, analizzare e presentare le prove digitali memorizzate, trasmesse e ricevute dai sistemi informatici e telematici. Il processo di investigazione digitale si articola in fasi ed attività racchiuse all'interno di modelli teorici che sono un valido supporto all'attività del *digital forensics expert* per il buon esito delle indagini. In questo articolo, l'autore presenta in ordine cronologico i modelli di investigazione digitale esistenti, analizzando le principali caratteristiche di ogni modello.

Digital forensic and digital investigation models

Digital forensic is a branch of forensic science that deals with identification, acquisition, analysis and presentation of the digital evidence stored, transmitted and received by computer and telecommunication systems. Digital forensic investigation process is divided into phases and activities within theoretical models that are a valuable support to the digital forensics expert for the success of the investigation. In this paper the author presents, in chronological order, an overview of existing digital forensic investigation models and analyzes the principal characteristics of each model.

Antonio Fiore