Ciberspazio e diritto 2013, Vol. 14, n. 49 (3-2013), pp. 345-359

Strumenti informatici di servizio ai cittadini stranieri: la banca dati normativa PAeSI

Mariasole Rinaldi[1]

Sommario: 1. Il progetto PAeSI e il servizio offerto – 2. Gli standard: regole condivise per la strutturazione dei documenti normativi – 3. Uno strumento per la redazione e la marcatura dei provvedimenti normativi – 4. La banca dati normativa

1. Il progetto PAeSI e il servizio offerto

Il progetto PAeSI (Pubblica Amministrazione e Stranieri Immigrati) nasce con l'intento di fornire un punto di accesso telematico unico per i servizi che vedono coinvolti amministrazioni pubbliche e stranieri residenti nel territorio toscano, ovvero un luogo dove gli operatori della pubblica amministrazione, che svolgono un ruolo di supporto informativo verso i cittadini stranieri, possano trovare informazioni aggiornate e dettagliate su procedure e normativa.

Il sito web del sevizio per l'immigrazione PAeSI[2], infatti, oltre a mettere a disposizione informazioni puntuali e aggiornate sui procedimenti amministrativi che coinvolgono i cittadini stranieri e le diverse amministrazioni, fornisce una banca dati aggiornata contenente la normativa italiana in materia di immigrazione.

[1] L'autrice è assegnista di ricerca presso l'Istituto di Teoria e Tecniche dell'Informazione Giuridica (ITTIG) del CNR.

[2] Il sito web è consultabile all'indirizzo www.immigrazione.regione.toscana.it, ma anche raggiungibile dalla sezione immigrazione del sito istituzionale della Regione Toscana (http://www.regione.toscana.it) e può essere richiamato dai numerosi siti territoriali quale comune punto di riferimento per la condivisione di informazioni complete e aggiornate su procedure amministrative e normativa influenti sulla condizione giuridica del cittadino straniero.

Il portale PAeSI è stato realizzato grazie alla collaborazione tra Regione Toscana (Direzione Generale Organizzazione e Sistemi informativi), Prefettura di Firenze (Consiglio Territoriale per l'Immigrazione) e Istituto di Teoria e Tecniche dell'Informazione Giuridica (ITTIG) del CNR.

In progetto è oggi inserito nel Piano di azione regionale "e.Toscana", che rappresenta un nuovo modo di fare amministrazione grazie all'apporto abilitante della tecnologia, delle infrastrutture e delle competenze proprie di una nuova società basata sull'informazione e la conoscenza.

Il sito PAeSI è in continua evoluzione: intende rendere sempre più accessibile l'interfaccia grafica al fine di facilitare i meccanismi di ricerca dell'informazione da parte dell'operatore dello sportello e amplia i contenuti informativi disponibili. Lo sviluppo del portale si pone l'obiettivo, infatti, di favorire la diffusione dell'informazione in ambiti tematici specifici come quelli relativi ad esempio alle opportunità di apprendimento della lingua italiana, rappresentando sempre di più uno strumento in grado di facilitare la circolazione delle informazioni sugli eventi di comune interesse.

Il tema dell'immigrazione risulta essere fortemente complesso e difficilmente comprensibile per gli utenti in generale, a maggior ragione rischia di esserlo per il cittadino straniero, che si trova immerso in un apparato amministrativo fortemente strutturato, talvolta con un livello di conoscenza della lingua italiana non sufficientemente alto da riuscire a districarsi all'interno del linguaggio giuridico specializzato. Proprio, infatti, il bisogno da parte della collettività di accedere facilmente ai dati giuridici da cui estrapolare informazioni precise che si sostanziano in procedimenti amministrativi, diventa di fondamentale importanza.

Gli utenti stranieri necessitano, quindi, di soggetti, identificabili negli operatori pubblici, che forniscano loro un'informazione "filtrata"; essi, infatti, dotati di una conoscenza globale della normativa e dei relativi procedimenti di competenza delle diverse amministrazioni[3], possono mediare l'informazione loro necessaria.

[3] Tra le diverse amministrazioni competenti in materia di immigrazione troviamo ad esempio le Prefetture, le Questure, i Comuni, le Camere di Commercio, le Direzioni provinciali del Lavoro del territorio toscano. Il sito web PAeSI, infatti, rientra nella cate-

Abstract

Strumenti informatici di servizio ai cittadini stranieri: la banca dati normativa PAeSI

Questo articolo si occupa della gestione dei documenti normativi e la loro pubblicazione sul Portale PAeSI (Pubblica Amministrazione e Stranieri Immigrati). Obiettivo del progetto PAeSI, infatti, è quello di offrire agli utenti un punto di accesso telematico unico alle informazioni su procedure e norme in materia di immigrazione. PAeSI è un portale web che consente agli utenti di consultare una banca dati normativa, implementata secondo le più avanzate tecniche di informatica giuridica, dotata di diverse funzioni di consultazione.
Le norme sono visualizzabili nel testo vigente, alle diverse date di modifica e nella versione multivigente, grazie alla strutturazione dei documenti secondo gli standard NiR: uno standard XML per la rappresentazione delle norme con relativo DTD (*Document Type Definition*) per rappresentare le diverse tipologie di provvedimenti ed uno standard per l'identificazione univoca delle norme stesse (URN). I documenti normativi sono trattati tramite lo strumento software *XmLeges-Editor*, sviluppato dall'Istituto di Teoria e Tecniche dell'Informazione Giuridica del CNR.

Advanced applications to support foreign citizens: the PAeSI normative data base

This article deals with the management and publishing of normative documents on the PAeSI Portal (Public Administration and Immigrants). The aim of the PAeSI project, in fact, is to offer users a single point of access to integrated information about procedures and norms in the immigration field. PAeSI is a web portal that allows users to query a data base of norms, implemented using the most advanced techniques of legal information, according to different modalities. Norms are visualized in the original text, at the different dates of modification and in the multi in-forced version, thanks to the structuring of normative provisions according to the NiR standards: an XML standard for the representation of norms with its DTD (*Document Type Definition*) to represent the different types ofnormative documents and finally a standard for unique identification of norms themselves (URN). Normative documents are processed by the software *XmLeges-Editor*, developed by the Institute of Legal Information Theory and Techniques of the Italian National Research Council (CNR).

Mariasole Rinaldi

Ciberspazio e diritto 2013, Vol. 14, n. 49 (3-2013), pp. 363-400

Lo sfruttamento del diritto d'autore tramite Internet

Luigi Cuomo[1]

Sommario: 1. Premessa – 2. La normativa sul diritto d'autore – 3. La circolazione delle creazioni intellettuali nelle reti telematiche – 4. L'evoluzione del diritto d'autore – 5. Il fenomeno della pirateria digitale – 6. Le forme di aggressione al diritto d'autore nelle reti telematiche – 7. Evoluzione normativa e strategie di contrasto alla pirateria – 8. Gli strumenti tecnici di contrasto alla pirateria – 9. Digital Rights Management e misure tecnologiche di protezione – 10. I nuovi modelli di distribuzione delle opere – 11. Le autorità preposte alla tutela del diritto d'autore – 12. Conclusioni

Il pensiero è come l'oceano,
non lo puoi bloccare,
non lo puoi recintare…

Lucio Dalla

1. Premessa

Nell'attuale società globalizzata l'interazione tra il diritto d'autore e la rete Internet rappresenta un modello di sviluppo di fondamentale importanza.

Il network globale ha una relazione strettissima con il diritto d'autore per la diffusione a distanza di contenuti creativi on-line (come musica, immagini, fotografie e filmati) assoggettati alla normativa sul copyright e, al contempo, per la protezione delle soluzioni tecniche adottate per costruire e potenziare l'architettura di rete.

La rete rappresenta un volano di crescita economica che riesce ad espandere pienamente la sua funzione commerciale solo per mezzo di innovativi modelli distributivi dei contenuti regolamentati da un sistema di diritti gestibili dai titolari delle creazioni intellettuali.

[1] Magistrato. Intervento all'incontro di studio sul tema: "La tutela della proprietà industriale e intellettuale" presso il Consiglio Superiore della Magistratura, Nona Commissione - Tirocinio e Formazione Professionale.

Internet è il centro informativo che rende prontamente disponibile agli utenti ogni genere di dati e di conoscenza: i servizi sono forniti sulla base dell'uguaglianza di accesso, senza distinzione di età, razza, sesso, religione, nazionalità, lingua o condizione sociale.

Internet si distingue dai mezzi di comunicazione tradizionali in quanto, pur utilizzando analoghe tecnologie di trasmissione, non offre al pubblico informazioni selezionate da intermediari, ma l'uso e i contenuti sono scelti direttamente da ciascun utente, che può trarre dalla rete ed al contempo immettervi ciò che vuole.

Il diritto d'autore è fondato sulla protezione automatica delle opere creative, sulla durata della privativa e sul principio di territorialità della tutela (estesa solo ai Paesi che hanno siglato trattati di reciprocità).

Internet non è territoriale e ogni server all'interno del quale sono digitalizzate le opere protette è accessibile da qualsiasi parte del mondo, i contenuti multimediali sono spesso di carattere temporaneo e le tecnologie di trasmissione sono costantemente in evoluzione.

L'interazione di Internet con il diritto d'autore rimane tuttora problematica, perché la rete ha una dimensione internazionale e i siti web presentano barriere di accesso molto basse e sono accessibili da qualsiasi computer in qualunque parte del globo, mentre il diritto d'autore rimane governato da ogni singolo Stato all'interno del proprio territorio.

Il quadro normativo internazionale del diritto d'autore, con modesti adattamenti succedutisi nel tempo, è riuscito a governare il settore fino alla diffusione della radio e della televisione per poi manifestare evidenti lacune e criticità con lo sviluppo delle tecnologie digitali e di Internet.

Solo di recente gli Stati Uniti, l'Unione Europea e gli altri Paesi industrialmente sviluppati hanno siglato accordi e trattati per la gestione dei diritti digitali, nella prospettiva di introdurre un regime legale per le opere multimediali divulgate on-line.

Gli Stati Uniti con l'adozione del Digital Millenium Copyright Act nel 1998 e l'Unione Europea con l'attuazione della Direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, hanno fatto transitare i contenuti diffusi su Internet nella sfera del diritto d'autore ed è stato sviluppato il commercio in rete dei prodotti tutelati dalle norme sulla proprietà intellettuale.

Abstract

Lo sfruttamento del diritto d'autore tramite Internet

L'articolo si propone di analizzare la trasformazione del diritto d'autore, che ha perso le sue caratteristiche tradizionali legate alla materialità della diffusione e alla territorialità delle forme di tutela. L'opera intellettuale viene attualmente creata, pubblicata, trasportata, diffusa e riprodotta direttamente attraverso "bit" senza alcun supporto materiale di estrinsecazione. Sono state, in particolare, analizzate le implicazioni giuridiche discendenti dalle forme di adeguamento della proprietà intellettuale allo sviluppo della rete e dalla introduzione di nuove tecniche di elaborazione, sfruttamento economico e utilizzazione delle creazioni immateriali.

The exploitation of copyright via Internet

The article sets out to analyze the transformation of copyright, which has shed its traditional characteristics bound up with the material nature of distribution and the territorial nature of its protection. Now, intellectual property is created, published, transported, distributed and reproduced directly through 'bit traffic' without any physical material support. In particular, those juridical implications are analysed that are rooted in the forms of adjustment of intellectual property to the development of the net and the introduction of new elaboration techniques, economic exploitation and the very use of immaterial creations.

Luigi Cuomo

Ciberspazio e diritto 2013, Vol. 14, n. 49 (23-2013), pp. 403-423

Identità digitale: tra esigenze di condivisione e necessità di tutela

Angelo Osvaldo Rovegno[1]

Sommario: 1 Introduzione – 2. Identità digitale come rappresentazione di se stessi – 3. Gestione dei dati di navigazione – 4. Provvedimenti del Garante per la Privacy in merito all'attività di profilazione degli utenti – 5. Estrapolazione di dati personali dalle preferenze espresse sui social network – 6. Diritto all'oblio – 7. Riconoscimento giurisprudenziale del "diritto all'oblio" – 8. Utilizzo dei dati personali per attività di monitoraggio della vita privata (il caso R.I.O.T.) – 9. Gestione dei dati personali da parte delle applicazioni mobili – 10. Identità digitale e accesso a sistemi informatici – 11. Sistema unificato di identità digitale – 12. Tutela penale dell'identità digitale

1. Introduzione

Uno degli aspetti forse più rilevanti connessi all'evoluzione di Internet è il tipo di utilizzo che ne viene fatto dagli utenti: da una forma di fruizione che inizialmente era quasi esclusivamente di consultazione passiva, si è via via passati ad un modello che prevede una crescente interazione con lo strumento, arrivando ad un utilizzo che contempla sempre più spesso l'inserimento di propri contenuti. Si pensi, per esempio, ai siti di hosting e fruizione di contenuti multimediali forniti dagli utenti, ai social network, ai blog, ai forum.

Questo riversare nella rete elementi riferibili alla propria persona e alla propria vita reale, unito inscindibilmente con l'ampliamento dell'accesso ad internet, ha portato ad un crescente interesse, non solo da parte degli utenti, ma anche delle Istituzioni, verso il tema della tutela dell'identità digitale, non tanto intesa nell'eccezione di credenziali di accesso ad un sistema informatico (delle quali comunque si parlerà oltre), quanto piuttosto di informazioni personali presenti in rete e riferibili ad un dato soggetto reale.

[1] Avvocato del Foro di Piacenza.

Sotto questo aspetto si pone il problema della gestione di quei dati che siano, di fatto, fonti di dati sensibili o comunque riferibili alla sfera privata del soggetto.

La questione non è di agevole approccio, posto che molto spesso questi dati sono volontariamente condivisi dal soggetto, anzi, spesso la loro condivisione è lo scopo stesso della loro pubblicazione (si pensi ai documenti multimediali caricati sui siti di hosting, o ai messaggi postati su blog, forum e social network). Quello che spesso avviene in modo meno consapevole è la reale quantità e qualità delle informazioni, e il loro eventuale utilizzo da parte di terzi, che l'inserimento di un file o di un post possono comportare.

Si pensi, per esempio, alla geolocalizzazione delle foto, che ormai molti apparecchi fotografici e smartphone sono in grado di effettuare, e della condivisione che di questi dati viene fatta, spesso in maniera inconsapevole perché attivata di default sul dispositivo o perché viene omessa un'adeguata valutazione delle reali conseguenze della condivisione indiscriminata delle coordinate geografiche della propria abitazione o del proprio luogo di lavoro.

Lo stesso dicasi della geolocalizzazione dei messaggi postati.

2. Identità digitale come rappresentazione di se stessi

Seppur relativamente nuovo il tema dell'identità digitale e dei problemi connessi alla sua tutela è di un certo interesse, soprattutto per le prospettive future connesse al suo utilizzo, strettamente correlate al volume di affari che ne può derivare.

La rappresentazione dell'immagine di noi stessi che forniamo sulla rete è sempre più accurata, e più lo diventa, maggiore è il valore, anche economico, che essa acquista.

Una ricerca svolta dal "Boston Consulting Group"[2] stima che il volume di affari correlato alla gestione delle identità digitali possa rag-

[2] Cfr. J. Rose, O. Rehese, B. Röber "The Value of our digital identity", b*gc.perspectives,* https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity/, (20/10/2013).

Abstract

Identità digitale: tra esigenze di condivisione e necessità di tutela

L'articolo si propone di analizzare l'evoluzione nell'utilizzo di internet e le problematiche connesse alla condivisione dei propri dati personali in relazione alle tematiche inerenti la privacy. A tale scopo vengono esaminati i risultati degli studi condotti dal "Boston Consulting Group" finalizzati alla quantificazione del valore economico attribuibile alle Identità Digitali e quelli dell'Università di Cambridge sull'estrapolazione di dati personali attraverso l'analisi delle preferenze espresse sui social network. Vengono anche presi in esame i nuovi indirizzi Comunitari sulla gestione dei dati di navigazione ed il riconoscimento del "Diritto all'Oblio". Viene esaminato il problema di possibili violazioni della privacy attuate tramite l'utilizzo di dati personali reperiti in rete, con particolare riferimento al "Caso R.I.O.T." nonché la tematica della gestione dei propri dati personali da parte delle applicazioni installate sui dispositivi portatili. Si passa all'analisi delle problematiche connesse alla personalità digitale intesa come credenziali di accesso a sistemi informatici con particolare riferimento alle "Identità Federate", per concludere con le novità di diritto interno sul sistema unificato di identità digitale e la tutela penale dell'identità digitale.

Digital identity: between sharing needs and needs for protection

The article aims to analyze the evolution in the use of internet and the issues related to the sharing of personal data in relation to aspects concerning privacy. For this purpose are examined results of studies conducted by the "Boston Consulting Group" aiming at quantifying the economic value attributable to Digital Identity and of the University of Cambridge on the extrapolation of personal data through the analysis of the preferences expressed on social networks. Are also taken into consideration the new Community lines on the management of the navigation data and the recognition of the "right to be forgotten". It examines the issue of possible privacy violations implemented through the use of personal information found on the net, with particular reference to the "RIOT case" as well as the theme of the management of personal data by the applications installed on mobile devices. Moves on to the analysis of issues related to digital personality meant as credentials to access to computer systems with particular reference to the "Federated Identity", to conclude with the national law news on the unified system of digital identity and the criminal protection of digital identity.

Angelo Osvaldo Rovegno

Ciberspazio e diritto 2013, Vol. 14, n. 49 (3-2013), pp. 427-445

Il *cyberterrorismo*: un'introduzione

Raffaella Pino[1]

Sommario: 1. Introduzione – 2. Il *cyberterrorismo* – 3. Le organizzazioni terroristiche e l'uso di Internet – 4. Esempi di attacchi terroristici – 5. Il *cyberterrorismo* e la risposta dal resto del mondo – 6. Conclusioni

1. Introduzione

L'invenzione e la repentina diffusione di Internet e delle nuove tecnologie[2] strettamente connesse alla rete (ad esempio la crittografia, lo scambio di file e d'informazioni, i protocolli di comunicazione, i siti web), negli ultimi dieci anni hanno trasformato completamente le relazioni sociali, le modalità di comunicazione e le organizzazioni della nostra società[3].

[1] Laureata in Giurisprudenza e perfezionata in computer forensics e investigazioni digitali presso l'Università degli Studi di Milano.

[2] Per "nuove tecnologie" si intendono le comunicazioni digitali (che permettono ai dati di essere compressi), i sistemi d'arma che possono sfuggire alla rilevazione radar (*stealth*), il sistema di posizionamento globale, GPS (che rende possibile una guida ed una navigazione più precisa) e l'*Information Technology* (IT), in particolare i nuovi strumenti per il recupero e l'analisi automatica dei dati, i *data* e il *text mining*. Cfr. A. Zanasi, "Information Warfare, Business Intelligence, Text Mining", in *Clusit.it,* relazione presentata ad *Infosecurity,* 12 Febbraio 2003. Disponibile all'indirizzo Internet http://www.clusit.it/infosecurity2003/zanasi.pdf (Consultato in data: 18.03.2013).

[3] È necessario affermare che da quanto appena dichiarato è possibile trarre due principali osservazioni: se da una parte Internet produce potenzialità comunicative e strumentali nuove (ad esempio per l'economia, la scienza e la medicina, la completa informatizzazione e l'accesso via Internet dei dati relativi ai donatori di midollo osseo su scala mondiale), dall'altra offre, in particolare alle organizzazioni terroristiche, un insieme di risorse immediatamente e magistralmente sfruttate per la loro lotta. Cfr. D. Tosini, "Terrorismo online: Internet e violenza nel XXI secolo", in *Equilibri,* anno XII, n. 2, Agosto 2008, pp. 193-206. Disponibile all'indirizzo Internet: http://www.domenicotosini.org/wp-content/uploads/2011/02/2008-Tosini-Terrorismo.Online-Equilibri.12.2.pdf (Consultato in data: 18.03.2013).

Di conseguenza, sono mutate completamente le condizioni e i metodi di impiego delle informazioni: qualsiasi utente può accedere alle informazioni e disporre di esse con più facilità, immediatezza e a basso costo (a volte gratuito), permettendo, così facendo, maggiori scambi comunicativi anche a grandi distanze. Per esempio, proprio questa altissima comodità di scambi di informazioni tutt'ora permette ai gruppi terroristici, anche se posizionati in luoghi o continenti diversi e distanti migliaia di chilometri, di interagire nell'anonimato attraverso l'uso di sofisticati sistemi di comunicazione (a titolo esemplificativo la steganografia viene utilizzata da Al-Qaeda per comunicare al meglio con i propri membri al fine di coordinare attacchi o fare proselitismo)[4], coordinando le loro attività e progettando operazioni terroristiche senza entrare in contatto fisico gli uni con gli altri e rendendo, quindi, gravosa l'attività investigativa[5].

Al giorno d'oggi, pertanto, la rete si sta espandendo e potenziando sempre più e con essa anche la criminalità che trova terreno fertile per realizzare nuovi crimini informatici: le minacce legate al cyberspazio, un nuovo "territorio" in grado di immagazzinare, modificare e scaricare informazioni, un "luogo" vasto e ancora poco conosciuto e frequentemente soggetto ad attacchi di terroristi informatici. La minaccia cibernetica col tempo ha conosciuto un progressivo potenziamento e miglioramento che gli ha conferito una dimensione strategica *ad hoc*: se da tempo si accostano ai singoli hacker[6] le organizzazioni terroristiche e criminali,

[4] Si noti che la steganografia è per sua natura un sistema ideale per usi criminali, soprattutto quando sia necessaria la massima segretezza. Avvalendosi di essa è possibile usare quasi ogni servizio di Internet come se fosse un *dead drop* (un luogo ben in vista, affollato usato dalle spie per mettere di nascosto del materiale – documenti, informazioni, fotografie, file.mp3 – in modo da permettere ad un'altra persona di prenderlo, evitando contatti diretti tra le parti) elettronico. Successivamente, il materiale potrà essere pubblicato tranquillamente all'interno di un *newsgroup* o in un sito Internet, poiché per chiunque potrà trattarsi solo di un'immagine o di un brano audio ma per il reale destinatario consisterà di un messaggio che attende solo di essere decodificato con un preciso codice o segnale. Cfr. E. Florindi, *Un approccio giuridico e tecnologico ai reati informatici*, Ed. Franco Angeli, Milano, 2005, pp. 180-189.

[5] Cfr. P. Galdieri, B. Negre, M. Strano (2002), *Cyberterrorismo. L'impiego delle reti telematiche da parte del terrorismo internazionale*, Jackson Libri, Milano, 2002. Disponibile stralcio anche in *Per Aspera ad Veritatem*, n. 23, maggio-agosto 2002, http://gnosis.aisi.gov.it/sito/Rivista23.nsf/ServNavig/37 (Consultato in data: 18.03.2013).

[6] Si tenga presente che con il termine hacker si intende un individuo anonimo e un assiduo combattente sedotto dal proibito. È un soggetto che non ama approfittare dei

Abstract

Il Cyberterrorismo*: un'introduzione*

L'articolo affronta una delle quattro categorie di crimini informatici esistenti che da tanto tempo minacciano il cyberspazio, il c.d. *Cyber-terrorismo*. Attraverso l'analisi di alcuni dei più significativi e memorabili attacchi terroristici verificatisi negli ultimi quindici anni, l'articolo mira ad evidenziare, in primo luogo, che i nuovi gruppi estremistici utilizzano questa nuova forma di violenza per progettare atti sempre più disastrosi e violenti al fine di seminare terrore, panico e mettere in serio pericolo fino, addirittura, a destrutturare una qualsiasi nazione in pochi minuti.
In secondo luogo, sottolinea che è di fondamentale importanza far apprendere alla popolazione mondiale questo nuovo tipo di attacco terroristico, attuando norme giuridiche mirate e predisponendo iniziative governative idonee a fortificare le infrastrutture deboli e nello stesso tempo capaci di contrastare ogni incidente informatico.

The Cyberterrorism: an introduction

The article deals with one of the four categories of existing computer crimes that threaten by long time cyberspace, the *Cyber-terrorism*. Through the analysis of some of the most significant and memorable terrorist attacks that occurred in the past fifteen years, the article aims to highlight, in the first place, that new extremist groups use this new form of violence to plan acts increasingly disastrous and violent in order to spread terror, panic and, indeed, put in serious danger until the demount of a nation in a few minutes.
In the second place, the article, shows that is essential to teach to world population this new kind of terrorist attack, by implementing targeted legal standards and by predisposing governmental initiatives suitable to fortify weak infrastructures and at the same time able to thwart every cyber incidents.

Raffaella Pino

Ciberspazio e diritto 2013, Vol. 14, n. 49 (3-2013), pp. 449-475

Attività di analisi forense su sistemi di *cloud computing*

Arianna Del Soldato[1]

Sommario: 1. Introduzione – 2. Il *cloud computing* – 3. L'analisi forense digitale – 4. L'analisi forense nel *cloud* – 5. L'analisi forense e le normative sulla nuvola – 6. Conclusioni

1. Introduzione

Il cloud computing è una innovazione tecnologica molto importante, che ha reso molto più efficiente la possibilità di accedere a dati, documenti e programmi a basso costo, da qualsiasi parte del mondo, anche grazie alla diffusione sempre più capillare dei dispositivi mobili e dei personal computer.

Questa nuova tecnologia ha, altresì, permesso di ridurre i costi di gestione, di migliorare la produttività personale e lavorativa e, forse, anche la qualità della vita degli utenti.

Il cloud computing introduce un nuovo modo di implementare architetture di tipo complesso e di realizzarle a basso costo, dunque accessibili facilmente da parte di aziende ma anche da privati.

La sua evoluzione è stata possibile grazie ai progressi avvenuti nel campo delle tecnologie di virtualizzazione delle macchine, alla disponibilità di connessioni a Internet a banda larga e di protocolli per l'interconnessione di sistemi eterogenei come i *Web services*. Ha, poi, sfruttato ampiamente un nuovo modo di utilizzare i servizi attraverso nuovi dispositivi mobili di ogni tipo. Tutto ciò ha contribuito alla sua rapida diffusione.

[1] Tecnologo presso l'Istituto di Informatica e Telematica del CNR di Pisa, Italia. Membro della Struttura di Servizio "Servizi Internet e Sviluppo Tecnologico" dello IIT-CNR e del Registro .it, si occupa della progettazione e sviluppo di applicazioni telematiche innovative e servizi per lo IIT, per il Registro .it e, più in generale, per il CNR e la Pubblica Amministrazione. Tiene corsi di formazione per specialisti e non del settore ed è autore di varie pubblicazioni.

Le caratteristiche e i benefici ottenuti utilizzando sistemi cloud hanno contribuito ad accumulare un numero sempre maggiore di dati digitali che rappresentano un patrimonio prezioso e una risorsa strategica per privati e aziende.

Insieme ai riconosciuti benefici sia in campo economico che sociale, è tuttavia opportuno rilevare come il cloud computing abbia evidenziato problemi concernenti la riservatezza e la sicurezza dei dati, nonché la permeabilità agli attacchi informatici. La creazione di grandi aggregazioni di dati ha generato obiettivi ben visibili e appetibili da parte di criminali informatici. Per questo motivo, il mondo investigativo dell'analisi forense digitale sui sistemi di cloud computing sta cercando di adeguare le procedure investigative standard a questo nuovo paradigma rendendolo, di conseguenza, affascinante anche dal punto di vista giuridico.

2. Il cloud computing

Cos'è il cloud computing? Il cloud computing è un termine che identifica un nuovo modo di fruizione di servizi IT.

Pur in difetto di una sua definizione univoca, appare particolarmente interessante la definizione fornita dal National Institute of Standards and Technology (NIST) che lo definisce come un «modello per abilitare un accesso pratico, "on-demand", via rete, a un insieme di risorse informatiche condivise (reti, Server, storage dei dati, applicazioni e servizi) e configurabili che possono essere rilasciate in tempo breve e con una minima gestione o interazione con il provider»[2]. Il concetto di cloud computing è caratterizzato da cinque peculiarità:

(1) Offerta di servizi on-demand che possono essere fruiti dall'utente in maniera indiretta e automatica;
(2) Accesso alle risorse distribuite tramite rete e senza limiti dalla piattaforma del *client*[3];

[2] Cfr. P. Mell, T. Grance, *The NIST definition of Cloud Computing*, NIST U.S. Department of Commerce – Special Publication 800-145, Gaithersburg MD, 2011, p. 2.

[3] Sistema hardware e software impiegato dall'utente per usufruire dei servizi di Cloud*:* personal computer, cellulari, tablet, Server.

Abstract

Attività di analisi forense su sistemi di cloud computing

Il cloud computing è un modello di elaborazione distribuito che consente l'accesso condiviso, mediante rete e su richiesta, a risorse configurabili e delocalizzate. Esso ha permesso di ridurre i costi di gestione, di migliorare la produttività personale e lavorativa e, forse, anche la qualità della vita degli utenti. Questo documento prende in esame i vari modelli di sviluppo e di servizio del cloud computing fornendone le definizioni e analizzandone i benefici e i problemi derivanti dal suo utilizzo. Successivamente, fornisce una panoramica sui vari aspetti tecnici e procedurali che caratterizzano l'analisi forense digitale approfondendo, in particolare, come le metodologie standard si applichino ai vari modelli del cloud computing, esaminando le possibili problematiche e fornendo possibili soluzioni. Infine, prende in considerazione le possibili problematiche incontrate dall'analista forense nel corso delle investigazioni su sistemi di cloud computing in relazione alle norme vigenti in materia.

Forensic analysis on cloud computing systems

Cloud computing is a model of distributed computing that enables shared and on demand access to configurable and delocalized resources, through the web. This model has allowed us to reduce operating costs, improve personal and work productivity and, perhaps, also the quality of life of users. This paper examines the various models of development and service of cloud computing, providing definitions and analyzing the benefits and the problems arising from its use. Subsequently, this paper provides an overview of the various technical and procedural aspects that characterize digital forensic analysis investigating, in particular, how standard methodologies are applied to the various models of cloud computing, by examining the possible issues and providing possible solutions. Finally, it takes into account possible problems encountered by the forensic analyst during investigations on cloud computing systems in relation with the current regulations.

Arianna Del Soldato

Ciberspazio e diritto 2013, Vol. 14, n. 49 (3-2013), pp. 477-514

La ricerca delle fonti di prova sulle reti di *cloud computing*: le nuove frontiere delle investigazioni digitali tra profili giuridici e questioni operative

Donato La Muscatella[1]

Sommario: 1. Il panorama tecnologico – 2. Il *cloud computing* – 3. Gli aspetti tecnici: a) la struttura del dato; b) l'acquisizione del dato; c) la posizione del dato – 4. I profili giuridici: a) la fonte di prova; b) il mezzo di acquisizione; c) l'attendibilità della prova; d) la cooperazione investigativa internazionale – 5. Le prospettive di sviluppo: a) rivoluzioni tecniche; b) evoluzioni normative

1. Il panorama tecnologico

L'introduzione di strumenti che consentono di accedere da qualunque punto del globo ai propri dati ha indubbiamente trasformato il modo di utilizzare le tecnologie informatiche.

Da un lato, infatti, potendo contare ovunque sui propri documenti – salva la disponibilità di una connessione alla rete – gli utenti hanno cominciato ad utilizzare meno i supporti di memorizzazione "tradizionali". Dall'altro, la conservazione in remoto di tali informazioni (talvolta associate a dati riservati) ha moltiplicato i dubbi degli esperti in tema di riservatezza e, al contempo, aumentato le difficoltà delle investigazioni digitali.

Tali metamorfosi sociali, hanno generato – come di frequente accade – veloci cambiamenti dell'agire criminale, che acquisisce più rapidamente di quanto si creda il nuovo sapere.

Non si tratta, però, di innovazioni senza precedenti.

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

La criminalità più "informatizzata", in realtà, faceva già buon uso delle tecnologie, avvalendosi degli strumenti offerti dall'informatica per comunicare in modo più sicuro o, semplicemente, trasportare le evidenze al di fuori dei poteri dell'Autorità Giudiziaria nazionale.

Si pensi allo scambio di materiale illecito tramite il Web. Da tempo ormai i soggetti coinvolti in questo tipo di attività si sono attrezzati per ostacolare le indagini ed evitare le conseguenze delle loro condotte.

È sufficiente rammentare come anni fa, sia balzato agli onori delle cronache il primo caso italiano di regista di filmati pedopornografici, ch'era solito immagazzinare i propri file su una schiera server situati all'estero ed insistenti nel territorio di molteplici giurisdizioni[2].

Una questione non così nuova, quindi, ma che s'arricchisce di problematiche procedurali aggiuntive, connesse in primo luogo alla posizione delle evidenze.

2. Il cloud computing

Negli ultimi anni, poi, si sono diffusi sempre più rapidamente, anche tra gli utenti del nostro Paese, i cc.dd. servizi di *cloud computing*[3].

Il termine inglese indica, secondo la letteratura più accreditata, uno schema per l'accesso decentralizzato ad un gruppo di risorse informatiche condivise e modulari, che possono essere rapidamente attivate con minima interazione con il fornitore di servizi[4]. In altre parole, si tratta di

[2] L'articolo che, all'epoca dell'arresto, descriveva la vicenda, parlava di un'organizzazione criminale svolta utilizzando "un sistema di siti web (una trentina) posizionati su provider internazionali e accessibili tramite un complicato giro di password, con un giro di clientela che arrivava fino all'Australia" (http://archiviostorico.corriere.it/2006/agosto/13/Italiano_produceva_film_pedofili_per_co_9_060813089.shtml).

[3] A titolo esemplificativo, può citarsi, tra i tanti articoli di stampa, *Il Sole 24 Ore* che, già il 22 febbraio 2012, titolava "Cloud computing, l'Italia è sesta al mondo come ambiente favorevole alla nuvola informatica".

[4] Il documento in lingua originale, testualmente, afferma "is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (cfr. T. Mell, P. Grance, *The NIST definition of cloud computing. Recom-*

Abstract

La ricerca delle fonti di prova sulle reti di cloud computing*. Le nuove frontiere delle investigazioni digitali tra profili giuridici e questioni operative*

La disamina, dopo una breve introduzione sulle caratteristiche tecniche dei diversi modelli di servizi cloud based, indaga gli aspetti operativi ed i profili giuridici che connotano lo svolgimento di investigazioni digitali su questo tipo di piattaforme.
L'analisi viene estesa, poi, alle forme di cooperazione investigativa internazionale tra gli organi inquirenti dei diversi Paesi – all'interno ed all'esterno dell'Unione Europea – e si conclude con un approfondimento delle più recenti prospettive di sviluppo, tecniche e normative, di questo specifico settore del diritto processuale penale.

The search for cloud-based digital evidence. The new frontiers of digital investigations between legal and operational issues

The essay, after a brief introduction on the technical features of the different models of cloud-based services, investigates the operational and legal aspects that distinguish the conduct of digital investigations over this kind of platforms. The analysis is then extended to the forms of international cooperation between the investigative bodies of various countries – inside and outside the European Union – and ends with a deepening of the latest development perspectives, both technical and legal, in this specific field of criminal procedure.

Donato La Muscatella

Ciberspazio e diritto 2013, Vol. 14, n. 49 (3-2013), pp. 515-536

Analisi forense di sistemi di *file sharing*

Maurizio Martinelli[1]

Sommario: 1. Introduzione – 2. La diffusione dei sistemi P2P – 3. Architetture delle reti P2P – 4. La disciplina della *Digital Forensics* applicata ai sistemi P2P – 5. Conclusioni

1. Introduzione

Sin dagli esordi della rete Internet, quando la rete si chiamava ancora DARPANET[2] (da DARPA – Defense Advanced Research Project Agency) ed era una rete sperimentale gestita e utilizzata principalmente dal Dipartimento della Difesa americano – DoD, i protocolli e i sistemi di *file sharing* hanno avuto ampia e larga diffusione. In alcuni casi, come ad esempio nel caso del protocollo FTP (*File Transfer Protocol*), essi si sono rivelati addirittura essenziali per il funzionamento della rete. Si pensi, in particolare, agli anni nei quali il protocollo DNS (*Domain Name System*) non era ancora stato ideato e implementato e il sistema di traduzione e associazione di un nome di una risorsa di rete al proprio indirizzo IP (meccanismo della risoluzione diretta) e, viceversa, dell'indirizzo IP al corrispettivo nome (meccanismo della risoluzione inversa) era basato sulla presenza di un unico file centralizzato, denominato HOSTS.TXT e gestito dallo Stanford Research Institute (SRI) in California, che veniva trasferito tra i nodi partecipanti alla rete tramite tipici meccanismi di

[1] Tecnologo presso l'Istituto di Informatica e Telematica del CNR di Pisa (IIT-CNR). Responsabile della Struttura di Servizio "Servizi Internet e Sviluppo Tecnologico" dello IIT-CNR e del Registro .it È responsabile scientifico di vari progetti e collaborazioni di ricerca aventi come tematica principale Internet, i suoi servizi e le sue potenzialità. Ha tenuto oltre 60 corsi di formazione per specialisti e non del settore ed è autore di oltre 90 pubblicazioni.

[2] Successivamente la rete DARPANET ha preso il nome di ARPANET. Nel 1984 è passata sotto la gestione della National Science Foundation (NSF) diventando una rete principalmente accademica e di ricerca e, alla fine degli anni '80, ha preso l'attuale nome di Internet divenendo, con il tempo, la rete a diffusione globale che oggi tutti conosciamo.

file sharing. La definizione delle specifiche del protocollo FTP nel giugno 1980, a cura di John Postel, con l'RFC[3] 765, consentì di formalizzare, nell'ambito delle specifiche del suddetto protocollo, le modalità di trasferimento del file HOSTS.TXT tra le organizzazioni facenti parte della rete. Tuttavia, la soluzione adottata, con il passare degli anni e con il conseguente aumento dei computer connessi alla rete e dei servizi disponibili, non si dimostrò adeguata e, soprattutto, scalabile. La definizione delle specifiche del protocollo DNS nel 1983, con gli RFC 882 e 883, a cura di Paul Mockapetris, un ricercatore dell'Information Science Institute – ISI – in California, e la loro revisione con gli RFC 1034 e 1035 del 1987, consentirono il superamento delle problematiche legate alla risoluzione dei nomi delle risorse di rete e dettero vita a quello che, dopo quasi 30 anni, costituisce ancora il servizio essenziale e fondamentale per il funzionamento della rete.

Oggi Internet è un fenomeno a diffusione mondiale ed è entrata prepotentemente nella vita quotidiana di ognuno di noi, cessando di essere uno strumento utile a una ristretta cerchia di ricercatori e accademici, per diventare un potente e polivalente strumento e mezzo di comunicazione di massa. Utilizzando una semplice, anche se riduttiva definizione, si può affermare che «any entity (household, individual or firm) is considered connected to the Internet if it has the capability of communicating with other entities, via the physical structure of the Internet»[4].

Tale trasformazione della rete ha comportato, necessariamente, che negli anni si modificassero e si evolvessero le modalità di utilizzo e di comportamento dei cosiddetti "internauti". Nomi quali Telnet, FTP, SSH, DNS, SMTP, ecc. sono dei perfetti sconosciuti per la maggior parte di coloro che si sono avvicinati alla rete negli ultimi anni, mentre non lo sono nomi quali Web (oggi nell'accezione più comune identificata, addirittura, con la rete stessa), Google, Youtube, Facebook, Twitter, ecc.

L'utente della rete non si può più definire "utente" nel senso di "utilizzatore" e "mero fruitore di un servizio", perché esso partecipa e collabora, con i propri contenuti, le proprie idee, i propri contributi, i pro-

[3] RFC è l'acronimo di Request for Comments. Costituiscono i documenti standard della rete Internet e sono rilasciati dall'Internet Engineering Task Force (IETF).

[4] Cfr. S. Greenstein, J. Prince, *The Practical Handbook of Internet Computing*, Chapman & Hall/CRC Press, Boca Raton, FL, 2004.

Abstract

Analisi forense di sistemi di file sharing

La *Digital Forensics* è un processo investigativo che fa uso di tecniche informatiche per identificare, acquisire, conservare e analizzare indizi o fonti di prova digitali. Nell'ambito del presente studio, è stata applicata la disciplina della *Digital Forensics* ai sistemi di *file sharing* e, in particolare, ai sistemi P2P che rappresentano, senza alcun dubbio, la tecnologia più efficiente, scalabile e con elevate garanzie di anonimato, per condividere e scaricare dalla rete materiale illegale. In particolare, è stata esaminata l'analisi forense del sistema eMule e sono stati impiegati gli strumenti *open source* eMuleReader™ e eMule MET Viewer, per analizzare un caso concreto di utilizzo della rete P2P.

Forensic analysis of file sharing systems

The *Digital Forensics* is an investigative process that makes use of computer techniques to identify, acquire, store, and analyze digital evidence or sources of evidence. In the present study, the *Digital Forensics* has been applied to file sharing systems and, in particular, to the P2P systems that are, without a doubt, the most efficient, scalable, and with high guarantees of anonymity, technologies to share and download illegal material from the network. In particular, we have taken into account the forensic analysis of the eMule system and we have used open source tools such as eMuleReaderTM and eMule MET Viewer to analyze an actual case of use of the P2P network.

Maurizio Martinelli