Ciberspazio e diritto 2013, Vol. 14, n. 48 (2-2013), pp. 183-209

Anonimato, identità personale e diritto di cronaca nel mondo telematico. La sentenza della Corte di Cassazione n. 5525/2012

Francesca Eusebi[1]

Sommario: 1. Anonimato e oblio. – 2. Diritto all'identità personale. – 3. Le recenti indicazioni in argomento della giurisprudenza di legittimità: la sentenza della Corte di Cassazione Sez. III, 05 aprile 2012, n. 5525. L'identità personale contestualizzata. – 4. L'incidenza della tecnologia. – 5. Conclusioni.

1. Anonimato e oblio

Di anonimato se ne parla in diverse materie, a partire dal diritto civile per i temi riguardanti il diritto d'autore, l'anonimato della madre e la protezione dei dati personali, ma lo si trova anche in diritto costituzionale per quanto riguarda la manifestazione del pensiero, in diritto penale quale aggravante di alcuni reati di minaccia e in diritto processuale penale per quanto riguarda le notizie anonime di reato[2].

Vi è una difficoltà a ridurre ad unità nozioni di anonimato abbastanza specifiche nelle loro connotazioni. Si pone la questione se non sia più realistico accettare la coesistenza di molteplici definizioni nel nostro sistema, pur non del tutto collimanti tra loro[3].

La nozione di anonimato è fornita in maniera esaustiva dalla l. 675/1996 e in seguito dal D.lgs. 196/2003 all'articolo 4, comma 1°, lett.

[1] Francesca Eusebi è laureata in giurisprudenza all'Università di Bologna.

[2] G. Gardini, *Le regole dell'informazione: principi giuridici, strumenti, casi*, Milano, Bruno Mondadori, 2009 p. 202.

[3] G. Tarello, *L'interpretazione della legge*, Milano, Giuffrè, 1980, p. 112: "È frequentissima, nelle legislazioni moderne, la presenza di tecnicizzazioni di un vocabolo rispettivamente diverse in diversi settori disciplinari o in relazione ad istituti diversi entro lo stesso settore".

n, il quale ha ripreso il considerando 26 della direttiva 95/46/CE definendo il dato anonimo quale «dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile», dove per dato viene inteso il dato personale riferibile ad una persona determinata[4].

È stato più volte affermato, anche dal Garante per la protezione dei dati personali, che non è sufficiente che il dato sia solo e semplicemente dissociato da un nominativo, essendo invece necessario che non si possa risalire in alcun modo all'identificazione dell'interessato.

L'impossibilità di risalire all'interessato va valutata in relazione al lavoro e al tempo necessari per rendere l'informazione identificativa di un soggetto determinato.

Quindi, solo laddove lavoro e tempo siano richiesti in misura irragionevole può dirsi di essere in presenza di un dato anonimo[5].

Una caratteristica fondamentale del dato anonimo è la sua relatività: il dato può essere anonimo per alcuni soggetti ma non per altri, come ad esempio per il personale amministrativo che tratta il dato del paziente ma non per il medico che lo ha in cura.

Il dato anonimo, inoltre, può essere tale per alcune funzioni ma non per altre.

Se ne deduce che la liceità dell'utilizzo del dato personale è determinata in relazione alle finalità di trattamento ed ai soggetti abilitati a fruirne.

La nozione di dato personale registra una vasta dilatazione concettuale, bisogna considerare come dato personale qualsiasi enunciazione relativa ad un qualsiasi oggetto: ad esempio l'informazione relativa ad un fatto, a un atto, ad uno stato, ad una caratteristica fisica, morale, intellet-

[4] Art. 2, lett. a) della direttiva 95/46/CE: l'interessato deve sempre essere una persona fisica, Per tale ragione, nel parere 4/2007 sul concetto di dati personali del Gruppo ex art. 29 si legge: "The definition in the Directive contains four main building blocks, which will be analyzed separately for the purposes of this document. They are the following ones: "any information", "relating to", "an identified or identifiable", "natural person". Tale requisito non è stato tuttavia recepito dal nostro legislatore, con una scelta senz'altro discutibile, ma ritenuta legittima dalla Corte di giustizia europea.

[5] G. Finocchiaro, *Alcune riflessioni sulle norme sul trattamento dei dati personali*, in *La legge sulla privacy dieci anni dopo*, G.F. Ferrari (a cura di), Egea, Milano, 2008, p. 1429.

Abstract

Anonimato, identità personale e diritto di cronaca nel mondo telematico. La sentenza della Corte di Cassazione n. 5525/2012

Nella "società dell'informazione" la capacità delle tecnologie digitali di produrre, manipolare e distribuire informazioni e la sempre più ampia diffusione dell'attività giornalistica svolta mediante testate telematiche ha posto nuovi problemi di natura giuridica riguardanti la tutela dell'identità personale e l'anonimato su Internet in quanto la rete ha una memoria illimitata.
L'interprete deve operare un nuovo bilanciamento tra tutela del diritto di informare (ed essere informati) e tutela on-line dell'identità personale, alla luce delle recenti indicazioni in argomento della Cassazione fornite con la sentenza n. 5525/2012.
La sentenza prende in considerazione nello stesso ambito di riferimento (tutela della privacy e attività giornalistica) tre fattispecie: oblio, rettifica, aggiornamento/integrazione.

Anonymity, personal identity and freedom of the press in the electronic world. The sentence of the Supreme Court no. 5525/2012

In the "information society" the ability of digital technologies to produce, manipulate and distribute information and the wider dissemination of journalistic turning heads by Telematics has set new legal issues regarding the protection of personal identity and the 'anonymity on the Internet, as the network has an unlimited memory.
The interpreter must make a new balance between protecting the right to inform (and be informed) and on-line protection of the personal identity, in light of recent Supreme Court provided guidance on the subject of the sentence no. 5525/2012.
The sentence takes into account in the same frame of reference (protection of privacy and journalistic activities) three situations: oblivion, updating / integration.

Francesca Eusebi

Ciberspazio e diritto 2013, Vol. 14, n. 48 (2-2013), pp. 213-240

La strada maestra dell'*open government*: presupposti, obiettivi, strumenti

Fernanda Faini[1]

Sommario: 1. Il rapporto dell'Italia con le nuove tecnologie. – 2. I presupposti da creare. – 3. L'amministrazione digitale aperta. – 4. Sistemi e programmi informatici: *cloud computing*, riuso, *software* libero. – 5. Dati pubblici: *open data* e trasparenza. – 6. Servizi e partecipazione: servizi in rete, *customer satisfaction*, *e-democracy*. – 7. L'*open government* e i suoi effetti.

1. Il rapporto dell'Italia con le nuove tecnologie

L'analisi dello "stato di salute" di cui godono le nuove tecnologie in Italia è obbligato punto di partenza per progettare strategie di innovazione nel nostro Paese. È necessario infatti misurarsi con la realtà attuale per valutare il grado di pervasività delle tecnologie nel tessuto della società e conseguentemente immaginare le condizioni da creare e le soluzioni da attivare.

In premessa, l'osservazione stessa dell'ingresso delle tecnologie nella società umana evidenzia l'impatto profondo e pervasivo che hanno su ogni aspetto individuale e sociale della vita. Ciò è dovuto alla crescita di informazioni disponibili e al facile accesso alle stesse per mezzo delle tecnologie e del *web*, che di conseguenza comportano cambiamenti profondi nell'acquisizione e trasmissione della conoscenza. Le tecnologie muta-

[1] L'Autrice è 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 con la Facoltà di Giurisprudenza dell'Università di Firenze, dove è cultore della materia "Informatica giuridica". Collabora come docente con Formez PA e altre realtà. Autrice di pubblicazioni e relatrice in convegni, seminari e conferenze in materia. Laureata con lode in Giurisprudenza all'Università di Firenze, attualmente frequenta il Master universitario di secondo livello "Management pubblico ed e-government" dell'Università del Salento.

no i rapporti fra individui, in quanto le relazioni diventano semplici e immediate e vengono abbattuti gli ostacoli della distanza territoriale e temporale. Le attività private e pubbliche si spostano dalla realtà fisica a quella virtuale e le rappresentazioni informatiche producono effetti giuridici. Rapidità, semplicità e immediatezza sono le nuove parole d'ordine nel rapporto fra individui reso possibile dal *web*.

Già queste poche riflessioni denotano la necessità di un'evoluzione della società che, seppur innescata dall'ingresso delle nuove tecnologie, in queste non si esaurisca, dato che si deve sostanziare altresì in un conseguente e necessario cambiamento di logiche e processi. L'introduzione delle tecnologie comporta un profondo cambiamento culturale e organizzativo che deve accompagnarsi a un ripensamento e una reingegnerizzazione degli strumenti e delle attività.

Per comprendere l'impatto dell'innovazione nella società italiana è opportuno esaminare la fotografia dei dati relativi al 2012 che ci consegna Istat[2], al fine di comprendere il rapporto che cittadini, imprese e istituzioni hanno con le tecnologie in Italia, in modo da poter attivare le conseguenti azioni necessarie.

I dati mostrano un Paese in cui l'innovazione non gode di buona salute, soprattutto alla luce del confronto con il contesto europeo e internazionale. Questa fotografia sbiadita suggerisce la necessità di interventi mirati a restituire tinte forti e a portare il Paese in un buono stato di salute.

Per quanto riguarda i cittadini italiani, se si analizzano le condizioni relative all'utilizzo delle tecnologie consistenti nel possesso di un pc e della connessione a Internet, il dato risulta particolarmente negativo. La percentuale di famiglie che hanno un pc non arriva al 60% (59,3%), scende al 55,5% per l'accesso a Internet e al 48,6% per quanto riguarda la con-

[2] I dati cui ci si riferisce sono quelli contenuti nel Comunicato stampa di Istat del 20 dicembre 2012 "Cittadini e nuove tecnologie", http://www.istat.it/it/archivio/78166 (01/06/2013), e nel Comunicato stampa di Istat del 18 dicembre 2012 "Le tecnologie dell'informazione e della comunicazione nelle imprese", http://www.istat.it/it/archivio/77714 (01/06/2013). Le informazioni del comunicato "Cittadini e nuove tecnologie", come si legge nella nota metodologica che riporta la strategia di campionamento e il livello di precisione dei risultati, sono tratte dall'indagine multiscopo "Aspetti della vita quotidiana". Nella nota metodologica del comunicato stampa relativo alle imprese, si precisa che le unità di rilevazione sono pari a 34.680 imprese rappresentative di un universo di 206.327 imprese che occupano complessivamente 8.108.377 addetti.

Abstract

*La strada maestra dell'*open government*: presupposti, obiettivi, strumenti*

Al fine di conferire alle amministrazioni pubbliche italiane fisionomia conforme alla società odierna, il necessario punto di partenza è l'analisi del rapporto attuale che il Paese ha con le nuove tecnologie. La fotografia consegnata dai dati Istat permette di delineare le condizioni necessarie per esplodere il potenziale innovativo delle nuove tecnologie e dare vita a un nuovo rapporto tra pubblico e privato. La società attuale esige un profondo cambiamento delle istituzioni che segua l'evolversi delle relazioni e dei mezzi di comunicazione a sua disposizione. A tale scopo sono necessarie azioni finalizzate a cittadini, imprese e pubblica amministrazione. Creati i presupposti nella società, si possono tracciare le linee di un governo adatto alla società contemporanea: l'*open government*, che basa le sue fondamenta su trasparenza, apertura, partecipazione, collaborazione.
Di quali strumenti deve dotarsi l'amministrazione pubblica per essere *open*? Le norme stesse delineano gli elementi necessari per quanto attiene ai sistemi, ai dati e ai servizi. Nella recente normativa italiana si delinea infatti il virtuoso "combinato disposto" costituito da *cloud computing*, riuso e *open source* e, nei rapporti con l'esterno, emerge il paradigma dell'apertura dei dati (*open data*) e dei servizi, creando relazioni improntate alla partecipazione e collaborazione degli utenti, fino al loro coinvolgimento nei processi decisionali per mezzo di strumenti di *e-democracy*.
Gli effetti della costruzione dell'*open government* italiano sono stimabili in consistenti risparmi di denaro e tempo, maggior efficienza e qualità, recupero di credibilità e fiducia nelle istituzioni. Le nuove tecnologie sono in grado di sprigionare l'intelligenza collettiva e tradursi in servizi inediti e nuove soluzioni. L'effetto finale sta nel guadagno complessivo del sistema Paese: percorrere la strada maestra dell'*open government* significa adottare una strategia per la crescita dell'Italia.

The high road of open government: requirements, purposes, instruments

The analysis of the current relationship that the country has with new technologies is the starting point in order to lend to the Italian public authorities an appearance in compliance with today's society. The picture delivered by Istat data sets the necessary conditions to show the innovative potential of new technologies and to create a new relationship between the public authorities and the private sector. Today's society requires a profound change of the institutions, to follow

the development of the relations and of communications medium at its disposal. For this purpose, it's necessary to start actions aimed at citizens, businesses and public administration. Once created the conditions in society, it would be possible to draw the lines of a government suitable to contemporary society: an "open government", based on transparency, openness, participation, collaboration.

What tools should adopt the public administration to be open? The rules themselves outline the necessary elements as regards systems, data and services. In the recent Italian legislation arises the virtuous "combined provision" consisting of cloud computing, reutilization and open source, while the standard of the opening of data (open data) and services stands out in the relations with the outside world. This creates relationships based on the participation and collaboration of users, up to their involvement in decision-making processes by means of e-democracy tools.

The effects of the construction of Italian open government are estimated at substantial savings in money and time, an improved efficiency and quality, the recovery of credibility and trust in institutions. The new technologies are able to unleash the collective intelligence and to arise in innovative services and new solutions. The final effect is the overall benefit for the whole Country: to walk the high road of open government means to adopt a strategy for the growth of Italy.

Fernanda Faini

Ciberspazio e diritto 2013, Vol. 14, n. 48 (2-2013), pp. 243-264

L'effettiva conoscenza dell'attività illecita da parte dell'hosting provider: normativa italiana e spagnola a confronto

Simone Bonavita, Stefano De Cristofaro

1. Le ragioni di un approccio comparatistico

Scrivere un testo sull'argomento non è indubbiamente cosa semplice: il panorama legislativo è in continua mutazione, e l'intervento di tribunali e legislatori rischia sempre di rendere obsoleto anche un testo che abbia visto la luce solo da poche settimane.

Tuttavia sembra interessante, alla luce di alcuni nuovi sviluppi, cercare di fare il punto sullo stato dell'arte con particolare riguardo al panorama italiano e spagnolo.

La scelta di una trattazione comparatistica tra le normative vigenti in Spagna ed in Italia nasce dall'attenzione di voler sottolineare la crescente necessità di armonizzazione delle normative nazionali all'interno del quadro di riferimento quantomeno europeo, e soprattutto evidenziare come la tracciatura di alcune linee comuni nella giurisprudenza comunitaria sia più che desiderabile.

Infatti, seppur entrambe le normative nazionali siano una traduzione diretta della medesima normativa, potremo notare come ciascun pae-

se abbia declinato in maniera del tutto differente il dettato del legislatore comunitario.

Non ce ne vogliano i gelosi sostenitori e rivendicatori di una sovranità nazionale piena e completa, ma in materie come quella in analisi, che per sua naturalezza spiega i suoi effetti senza troppo badare ai confini nazionali, sembra auspicabile, nell'ottica di una certezza del diritto, una maggior armonizzazione e omogeneizzazione dei regimi nazionali europei.

Chiunque conosca o possegga nozioni basilari circa l'architettura e il funzionamento della Rete, saprà quanto delicato possa essere il ruolo degli Internet service provider, termine che identifica realtà molto diverse tra loro, sia per "dimensione" che per profilo – basti ricordare a titolo esemplificativo la distinzione tra "hosting attivo" e "hosting passivo" operata da parte della dottrina e della giurisprudenza, che non trova tuttavia risconto nella Direttiva Europea 2000/31/CE ("Direttiva sul commercio elettronico").

2. La disciplina europea della responsabilità dell'hosting provider

Per affrontare, in chiave comparatistica, il tema in argomento appare utile partire dalla responsabilità dell'hosting provider, come definita dalla Direttiva, Prevede la stessa, all'art. 14:

"1. *Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore*:

a) *non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione*;

b) *non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso*.

2. *Il paragrafo 1 non si applica se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore.*

Abstract

L'effettiva conoscenza dell'attività illecita da parte dell'hosting provider: normativa italiana e spagnola a confronto

L'articolo si occupa di una trattazione comparatistica tra le normative vigenti in Spagna ed in Italia sul tema della eventuale responsabilità del provider di contenuti e di servizi in Internet. L'analisi muove all'interno del quadro di riferimento europeo, e evidenzia come la tracciatura di alcune linee comuni nella giurisprudenza comunitaria possa essere più che auspicabile.
Ognuno dei due Paesi ha infatti declinato in maniera del tutto differente il dettato del legislatore comunitario.

The hosting provider's actual knowledge of illegal activity: a comparison between Italian and Spanish Law

The article deals with a comparative discussion between the laws in force in Spain and Italy on the subject of liability of providers of content and services on the Internet. The analysis moves within the European framework, and shows how the tracing of some common lines in Community law it is most desirable.
Each of the two Countries has, in fact, regulated in a completely different way the principles coming from the Community legislature.

Simone Bonavita
Stefano De Cristofaro

Ciberspazio e diritto 2013, Vol. 14, n. 48 (2-2013), pp. 265-275

La conservazione dei documenti in cloud computing

Guglielmo Troiano[1]

Sommario: 1. Premessa. – 2. Oggetti e soggetti. – 3. Privacy e sicurezza. – 4. Standard, formati e interoperabilità.

1. Premessa

La gestione documentale informatizzata all'interno delle strutture private è consolidata ormai da anni. Già nel 1997 [con il d.P.R. del 10 novembre 1997 n. 513, derivante dalla c.d. «legge Bassanini»], la normativa statale confermava il pieno valore giuridico dei documenti informatici.

In tempi recenti, i sistemi di cloud computing sono stati poi determinanti in relazione ai processi di condivisione e conservazione, sviluppando flussi e archivi documentali gestiti completamente online.

I vantaggi sono evidenti e comprovati ma non si possono sottacere gli aspetti negativi, anzi, la loro valutazione costituisce una necessaria attività per creare maggiore affidamento e consapevolezza negli utenti.

La specifica natura del cloud computing comporta infatti che le informazioni vengano trattate e conservate in contesti esterni al perimetro della propria rete aziendale e del proprio dispositivo elettronico, per cui, i rischi devono essere attentamente valutati in relazione ai modelli di servizio che si intende adottare ma, soprattutto, se si coinvolgono dati di terzi soggetti nell'esercizio di un'attività professionale.

Salvo il caso in cui si tratti di una società altamente specializzata che ha predisposto clausole contrattuali ad hoc per l'offerta di un ser-

[1] Avvocato del Foro di Milano, consulente della Community for Security di Oracle Italia, membro e ricercatore della Cloud Security Alliance Italy e cultore di Informatica Giuridica presso l'Università degli Studi di Milano.

vizio specifico di conservazione (sostitutiva), appare assai difficile far rientrare la complessa relazione tra azienda e outsourcer nei generici e standardizzati contratti di servizi di cloud computing che il mercato offre. Per cui, occorre cautela nella scelta del fornitore del servizio.

2. Oggetti e soggetti

La disciplina sui documenti informatici e la loro conservazione è contenuta nel Codice dell'Amministrazione Digitale (CAD), che prescrive le norme di carattere generale, e nelle regole tecniche[2] predisposte dal CNIPA[3].

I concetti essenziali da considerare sono:

- *documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;*
- *memorizzazione: processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici (o documenti informatici derivati) e documenti informatici, anche sottoscritti;*
- *archiviazione: processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti;*
- *conservazione: processo di "suggellamento" dei documenti informatici.*

Per essere giuridicamente rilevante, non occorre che al documento informatico sia legata una delle firme informatiche[4] attualmente previste

[2] DPCM del 22 febbraio 2013 "*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*" (GU n.117 del 21-5-2013) e Delibera n. 11 del 19 febbraio 2004, "*Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali*".

[3] Poi DigitPA e Agenzia per l'Italia Digitale.

[4] Il CAD riconosce la rilevanza di cinque tipologie di scritture private informatiche: i) il documento informatico privo di firma; ii) il documento informatico con firma elettronica; iii) il documento informatico con firma elettronica avanzata; iv) il documento informatico con firma elettronica qualificata; v) il documento informatico con firma digitale. A queste cinque tipologie di documento informatico rilevante in ambito "pri-

Abstract

La conservazione dei documenti in cloud computing

I sistemi di cloud computing sono diventati determinanti in relazione ai processi di condivisione e conservazione dei dati, sviluppando flussi e archivi documentali gestiti completamente online.
I vantaggi sono evidenti e comprovati ma non si possono sottacere gli aspetti negativi, anzi, la loro valutazione costituisce una necessaria attività per creare maggiore affidamento e consapevolezza negli utenti.
La specifica natura del cloud computing comporta infatti che le informazioni vengano trattate e conservate in contesti esterni al perimetro della propria rete aziendale e del proprio dispositivo elettronico, per cui, i rischi devono essere attentamente valutati in relazione ai modelli di servizio che si intende adottare ma, soprattutto, se si coinvolgono dati di terzi soggetti nell'esercizio di un'attività professionale. Questi sono i temi trattati nel presente articolo.

Documents storage with cloud computing

The cloud computing systems have become crucial in relation to the processes of sharing and storage of data, developing flows and document archives managed completely online. The advantages are obvious and proven but in this Article are mentioned the negative aspects too.
The specific nature of cloud computing means in fact that the information is processed and stored in contexts outside of the perimeter of the company network and its electronic device, so, the risks should be carefully considered in relation to service models to be adopted but especially if they involve third-party data subjects in the exercise of a professional activity. These are the topics discussed in this article.

Guglielmo Troiano

Ciberspazio e diritto 2013, Vol. 14, n. 48 (2-2013), pp. 277-294

Analisi forense di sistemi operativi Linux

Stefano D'Ambrosio[1]

Sommario: 1. Introduzione. – 2. I sistemi GNU/Linux. – 3. Organizzazione del file system. – 4. Analisi della configurazione del sistema. – 5. Analisi dei log. – 6. Account utente. – 7. File di swap. – 8. Analisi del file system. – 9. Conclusioni.

1. Introduzione

La metodologia di analisi forense di un sistema operativo GNU/Linux segue sostanzialmente gli standard e le *best practices* in uso nella digital forensics, ma per poter applicare correttamente questa metodologia, in particolare in fase di identificazione, acquisizione e analisi, è necessario conoscere le caratteristiche, le potenzialità e le criticità dello specifico sistema.

In questo articolo si vogliono mettere in evidenza le principali peculiarità di un sistema GNU/Linux, dal punto di vista della digital forensics.

Il tema è molto vasto: non è possibile trattarne in poche righe i vari aspetti; per questo viene fatto qui un rapido *excursus* solo di alcuni di essi, con lo scopo di dare le informazioni essenziali sul sistema e le principali problematiche.

Data la rapida evoluzione dei sistemi operativi e degli strumenti software, i riferimenti a dettagli tecnici citati nel testo possono facilmente diventare obsoleti: rimangono comunque valide le considerazioni di carattere generale e la metodologia di analisi.

[1] Ingegnere informatico e consulente tecnico per il Tribunale di Como.

2. I sistemi GNU/Linux

I sistemi operativi GNU/Linux sono costituiti da un kernel Linux, una serie di librerie di sistema e un insieme di strumenti software di base, che servono per effettuare le operazioni essenziali (installazione/aggiornamento del sistema stesso, gestione del desktop, manipolazione del file system, accesso alla rete ecc.). A questi software base vengono aggiunte applicazioni per i più svariati utilizzi.

Tutti questi componenti, opportunamente "pacchettizzati", costituiscono una distribuzione del sistema GNU/Linux[2].

Esistono centinaia di distribuzioni GNU/Linux[3], sia di tipo *general purpose*, che create per soddisfare esigenze in specifici campi di applicazione (desktop, server, forensics, sistemi embedded ecc.).

Nel 2006 è stato definito lo standard LSB (*Linux Standard Base* - ISO/IEC 23360), mirato a regolamentare le caratteristiche e la struttura interna delle distribuzioni basate su Linux.

Le distribuzioni più diffuse, aderendo in tutto o in parte a questo standard, presentano perciò alcune caratteristiche comuni a livello di organizzazione del file system, comandi di base, librerie di sistema ecc., che consentono dal punto di vista della digital forensics di orientare l'analisi in modo più mirato e definire alcune linee guida specifiche per l'ambiente GNU/Linux.

3. Organizzazione del file system

L'organizzazione del file system di un sistema GNU/Linux è definita dalle specifiche FHS (Filesystem Hierarchy Standard[4]), rispettate in linea di massima da tutte le principali distribuzioni. La gerarchia di directory è essenzialmente la seguente:

[2] Cfr. A. Ghirardini, G. Faggioli, *Computer Forensics*, Apogeo, Milano, 2007, pp. 272-274.

[3] Cfr. http://distrowatch.com (28/05/2013).

[4] Cfr. http://en.wikipedia.org/wiki/Filesystem_Hierarchy_Standard (28/05/2013).

Abstract

Analisi forense di sistemi operativi Linux

I sistemi basati su Linux si prestano molto bene per essere utilizzati come strumenti nell'ambito della *digital forensics:* esistono varie distribuzioni specifiche per questo scopo (DEFT, CAINE ecc.) e un numero enorme di *tool* che coprono praticamente ogni esigenza. Ma come affrontare il caso in cui il sistema Linux è l'*oggetto* dell'analisi? In questo articolo vengono evidenziate alcune caratteristiche specifiche dei sistemi GNU/Linux, che risulta utile conoscere in fase di acquisizione e analisi forense. Introduce in particolare all'analisi della configurazione del sistema, per individuare dove i dati di interesse possono essere trovati.

Forensics analysis of Linux operating systems

The Linux-based systems are well suited to be used as tools in the context of digital forensics: there are several specific distributions for this purpose (DEFT, CAINE etc.) and a huge number of tools for covering virtually every need. But how to deal with the case in which the Linux system is the *object* of analysis? This article highlights some specific features of the GNU/Linux systems, which are useful in the process of acquisition and forensics analysis. It introduces, in particular, the analysis of the system configuration, from which to draw a lot of information about where the data of interest can be found.

Stefano D'Ambrosio

Ciberspazio e diritto 2013, Vol. 14, n. 48 (2-2013), pp. 295-311

Computer forensics e fraud investigation

Francesco Firullo[1]

Sommario: 1. Introduzione. – 2. Fraud investigation e digital forensic. – 3. La fraud prevention.

1. Introduzione

Lo scopo del seguente lavoro è quello di illustrare l'utilità della c*omputer forensics* in ambito *corporate* e in particolare nell'ambito di quelle attività investigative volte a individuare le frodi aziendali.

Inizialmente è importante comprendere cosa si intende per *computer forensics.* Con tale termine si fa in genere riferimento alla «disciplina che studia l'insieme delle attività che sono rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova»[2]. Come si vedrà in seguito, questa disciplina col tempo ha assunto particolare rilevanza ai fini delle investigazioni interne aziendali.

Oggi le imprese sono sempre più esposte al rischio di incorrere in frodi aziendali e finanziarie di vario genere poste in essere anche da soggetti di elevato *status* sociale che operano all'interno e/o all'esterno di esse. Sempre più spesso si sente parlare di *white collar crime*, ossia di crimini commessi da individui di elevato livello culturale, nell'esercizio della propria attività professionale. Ciò in quanto, le frodi più sofisticate, compiute ad esempio mediante l'alterazione dei bilanci o l'utilizzo di complessi strumenti finanziari (ad es. strumenti finanziari derivati), ven-

[1] CONSOB, Milano. Le opinioni dell'Autore sono espresse a titolo personale e non impegnano in alcun modo l'Autorità di appartenenza.

[2] Cfr. G. Ziccardi, *Informatica Giuridica. Privacy, sicurezza informatica, computer forensics e investigazioni digitali*, vol. II, Giuffrè, Milano, 2012, p. 253.

gono architettate da soggetti che dispongono di «adeguate, approfondite e ben solide competenze»[3].

La maggior parte delle frodi perpetrate nel tempo sono state in genere realizzate attraverso schemi di attuazione relativamente consolidati e ripetuti nel tempo, che vengono classificati in tre macrocategorie principali – appropriazione indebita, falsi documentali, corruzione – a loro volta scomponibili in diverse sottocategorie (dando così origine a uno schema, che in ragione della sua rappresentazione grafica, viene definito «albero delle frodi»)[4].

Oltre agli schemi «elementari» di frode esistono schemi fraudolenti più complessi, implementati attraverso strutture societarie articolate e complesse (ad es. frodi carosello, riciclaggio di denaro proveniente da attività illecite, schemi di *re-billing*, frodi con parti correlate ecc.)[5].

Oltre al rischio per un'impresa di incorrere in uno degli schemi di frode di cui sopra, va oggi considerato anche il rischio di essere vittima di tutta una serie di attività fraudolente di «nuova generazione» poste in essere attraverso le nuove tecnologie informatiche (in particolar modo attraverso Internet) meglio note con il termine di *cybercrime*. Il *phishing,* il *pharming,* il *denial of service* sono tipici esempi di frodi poste in essere attraverso il web, definite anche come *internet fraud*[6].

Tra le varie frodi informatiche esistenti il *phishing* in italia è stato di recente oggetto di particolare attenzione. A causa dei numerosi attacchi subiti dai correntisti di rinomati istituti di credito la Procura di Milano (nel periodo giugno 2005 - agosto 2006) ha condotto un'indagine evidenziando che molto spesso le operazioni di *phishing* si strutturano attraverso operazioni di riciclaggio delle somme sottratte alle vittime[7]. Il fenomeno in questione desta tuttora forti preoccupazioni. «Le mail di *phishing* sono sempre più mirate e credibili». Inoltre, secondo i dati diffusi

[3] Cfr. G. Pogliani, N. Pecchiari, M. Mariani, *Frodi Aziendali*, Egea, Milano, 2012, p. 5 e ss.

[4] Cfr. *ivi*, p. 68.

[5] Cfr. *ivi*, p. 154 e ss.

[6] Cfr. *ivi,* p. 120 e ss.

[7] Per maggiori approfondimenti sulla tecnica del *phishing* cfr. F. Cajani, G. Costabile, G. Mazzaraco, *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria,* Giuffrè, Milano, 2008.

Abstract

Computer forensics e fraud investigation

L'articolo si propone di dimostrare l'utilità della *computer forensics* nell'ambito delle attività investigative volte ad individuare le frodi aziendali. Dopo un'analisi introduttiva sui principali schemi di frode esitenti, vengono analizzate le tecniche e gli strumenti di norma utilizzabili nelle fasi di acquisizione, estrazione ed analisi delle evidenze digitali. Successivamente vengono esaminate alcune tecniche di estrazione di dati, meglio note con il termine di *data mining,* che possono rivelarsi particolarmente utili nell'ambito di una *fraud investigation.* In particolare viene approfondita la tecnica della "*Social Network Analysis"*. Da ultimo viene affrontato il tema della *fraud prevention*, evidenziando come il fenomeno delle frodi aziendali possa essere mitigato attraverso l'implementazione di un sistema di *Enterprise Risk Management* e di un'attività di *fraud risk assessment*.

The article shows the utility of computer forensics in the area of investigation activities aimed at identyfying corporate fraud. After an introductory analysis of the main schemes of existing fraud, the Author analyses the techniques and the instruments used in the acquisition, extraction and analysis of digital evidence. Later some techniques of data extraction, better known as *data mining,* are examined. These tecniques can be particulary useful in a *fraud investigation*. In particular, the technique of *Social Network Analysis* is deepened. Finally the topic of *fraud prevention* is discussed, highlighting how the phenomenon of corporate fraud can be mitigated through the implementation of an *Enterprise Risk Management* system and by a *fraud risk assessment* activity.

Francesco Firullo

Ciberspazio e diritto 2013, Vol. 14, n. 48 (2-2013), pp. 313-330

Steganografia e steganalisi: occultamento di documenti aziendali e ricerca degli stessi utilizzando strumenti open source. Un caso reale

Romualdo Lo Rizzo[1]

1. Steganografia e steganalisi

La parola steganografia deriva dai termini greci *kryptos* (nascosto) e *graphein* (scrivere), per cui, come l'etimologia suggerisce, essa rappresenta una tecnica per nascondere informazioni.

La steganografia non è però solo l'arte di occultare un messaggio segreto, o presunto tale, all'interno di una comunicazione pubblica che sembrerebbe veicolare tutt'altra informazione, ma è anche la scienza di nascondere che la comunicazione abbia avuto luogo.

L'uso tipico della steganografia è quello di inviare o ricevere messaggi senza suscitare sospetti e quindi comunicare superando dei controlli e i suoi utilizzatori di norma sono spie, agenti segreti, terroristi, dipendenti infedeli.

È forse per questo che, nel campo dello spionaggio industriale come del terrorismo, purtroppo, si tende a usare la steganografia. Sapere a priori che un messaggio è crittografato mette subito in allerta gli investigatori informatici e gli esperti di codici segreti, mentre un messaggio steganografato può passare inosservato, senza destare alcun sospetto.

[1] Consulente Informatico perfezionato in Digital Forensics, amministratore della Informatica Sistemi Salento.

Spesso la steganografia viene accostata alla crittografia ma, in realtà, si tratta di due tecniche molto differenti. Mentre lo scopo della seconda è nascondere il contenuto di un messaggio, quello della prima è di occultare l'esistenza del messaggio stesso. Per raggiungere risultati ottimali, le due tecniche possono essere combinate: il messaggio da nascondere viene prima cifrato e poi gli si applica la steganografia.

La steganografia ha di positivo che si vuole nascondere il fatto stesso di stare comunicando con qualcuno, indipendentemente dal tipo di messaggio trasmesso, mentre, contrariamente a quanto accade con la crittografia, l'intercettazione mette a rischio il messaggio stesso.

Padre della steganografia è considerato l'abate Giovanni Tritemio (1462-1516) autore di due trattati sull'argomento, "Steganographia" e "Clavis Steganographiae", nei quali egli spiega come comunicare un messaggio segreto, nascondendolo in un testo a prima vista normale e quasi privo d'interesse.

1.1. Esempi storici

Una vecchia storia, ambientata alcuni secoli prima di Cristo, ci proviene dalle scritture di Erodoto. Il mezzo di scrittura del tempo era costituito da tavolette di legno ricoperte da cera sulla quale si incidevano i messaggi. Un esule greco stabilitosi in una città persiana, avendo saputo che Xerxes, re dei persiani, voleva invadere la Grecia, nonostante fosse in esilio, trovò uno stratagemma per avvisare i suoi compatrioti: sollevò la cera da una di queste tavolette, incise la notizia sul legno sottostante e la ricoprì nuovamente di cera. La tavoletta che conteneva il messaggio appariva come inutilizzata, così riuscì ad oltrepassare le ispezioni e a raggiungere i greci.

Sempre Erodoto narra che, per comunicare *segretamente,* si tatuava sulla testa rasata di qualcuno, di norma erano schiavi, il messaggio da recapitare. Appena ricresciuti i capelli questi umani raggiungevano il destinatario che, dopo aver provveduto a rasare di nuovo i loro capelli, aveva a disposizione quanto celato sotto di essi.

Si dice che il filosofo Aristotele comunicasse con il nipote Callistene, storico al seguito di Alessandro Magno durante la sua spedizione in Asia, attraverso manoscritti aventi argomentazioni futili e piuttosto gene-

Abstract

Steganografia e steganalisi: occultamento di documenti aziendali e ricerca degli stessi utilizzando strumenti open source. Un caso reale

Lo scopo della steganografia é quello di nascondere messaggi in immagini, filmati, file sonori, file di testo ed altri oggetti digitali detti contenitori. La steganalisi é l'arte di individuare i contenuti nascosti e, possibilmente, di svelarli. Con l'ausilio di tecniche di Digital forensics e di C.A.IN.E.(Computer Aided Investigative Environment), una distribuzione forense Open Source derivata da Ubuntu che integra, in un'interfaccia user friendly, molti dei tools forensi esistenti mettendoli a disposizione del digital forensic expert, si condurrà un'attività investigativa preventiva, ex art. 391 *nonies* del c.p.p. allo scopo di reperire delle evidenze digitali che possano avere valenza di prova in un probabile giudizio per spionaggio industriale.

Steganography and steganalysis: hiding of business documents and looking for the same using open source tools. A real case

The aim of steganography is to hide messages inside images, movies, audio files, text files and other digital objects called containers. Steganalisys is the art of detecting hidden messages and, possibly of decoding them. A precautionary investigative activity will be carried, ex art. 391 *nonies* c.p.p in order to trace digital facts that could be used as evidence in prospective trials for industrial intelligence/spying through the techniques of Digital Forensic and C.A.IN.E. (Computer Aided Investigative Environment), a forensic Open Source distribution derived from Ubuntu which completes, in a user friendly interface, many current forensics tools at disposal of the digital forensics expert.

Romualdo Lo Rizzo

Ciberspazio e diritto 2013, Vol. 14, n. 48 (2-2013), pp. 331-341

Analisi della RAM nella digital forensics

Francesco Zucconi[1]

Sommario: 1. Introduzione. – 2. Analisi della RAM. – 3. Dump. – 4. Alcuni tool di analisi RAM. – 5. Conclusioni.

1. Introduzione

L'argomento trattato fa parte di quella branca della scienza definita con il nome di *computer forensics* che si occupa dell'individuazione, estrazione, conservazione e protezione del dato informatico al fine di farlo valutare nel corso di un contesto giuridico[2].

Tale disciplina studia, inoltre, le tecniche e gli strumenti per l'esame dei sistemi informatici[3].

Le informazioni, una volta acquisite, dovranno essere trattate seguendo una metodologia ben precisa tramite la quale si dovranno acquisire le prove, autenticarle e analizzarle, senza che queste vengano danneggiate nel corso dei vari passaggi appena descritti.

I dati raccolti dovranno essere congelati in modo da poter essere analizzati in un secondo momento.

In base alla tipologia di analisi che dovrà essere effettuata si adopereranno strumenti, metodi e mezzi differenti.

Nel panorama complessivo si possono individuare due diverse tipologie di metodi di raccolta dati:

Memory analysis: si occupa di analizzare il supporto che non è più in funzione. Al suo interno sono memorizzate delle informazioni che potranno essere utili nel corso delle indagini. Solitamente è l'analisi fatta sull'hard disk del computer, dopo che questo è stato sequestrato;

[1] Laureato in Ingegneria, esperto di Ingegneria Forense, Perfezionato in Computer Forensics e Investigazioni Digitali.

[2] Cfr. Wikipedia, http://it.wikipedia.org/wiki/Informatica_forense

[3] Cfr. M. Epifani, http:// www.associazionearchimede.it/Unisa/phocadownload/ssi2011.pdf, 2011.

Live analysis: analisi che deve essere realizzata sulla scena del crimine, prima che venga tolta l'alimentazione elettrica al dispositivo, e vengano quindi persi i dati temporanei.

2. Analisi della RAM

L'analisi della RAM rientra nella *Live analysis* a causa delle sue peculiarità, che saranno di seguito descritte.

Il termine RAM è un acronimo usato in informatica che significa *Random Access Memory*: si tratta di un supporto di memoria sul quale è possibile leggere e scrivere informazioni con un accesso "casuale", ossia senza dover rispettare un determinato ordine, come ad esempio avviene per un nastro magnetico; il tempo necessario per leggere o scrivere un *bit* di memoria è indipendente dalla sua locazione.

Le RAM appartengono alla famiglia delle RWM (*read/write memory*) che sono dei registri di memoria all'interno dei quali è possibile scrivere e richiamare informazioni in qualsiasi istante.

Al contrario degli *hard disk*, dove i dati sono trascritti in maniera duratura e possono essere cancellati (solitamente solo con azione manuale), nella RAM i dati vengono memorizzati, fino ad occupare lo spazio a disposizione e cancellati del tutto o quasi, al momento dello spegnimento del computer.

Le RAM hanno ormai soppiantato le cosiddette memorie ad accesso seriale, nelle quali le locazioni di memoria sono sempre accessibili, ma richiedono un insieme di passi per essere lette.

La RAM è, perciò, la memoria principale di tutte le architetture *hardware*, sia a singolo processore sia multiprocessore.

Il processore (CPU) carica dalla RAM, quando non presenti nella propria *cache*, le istruzioni da eseguire e i dati da elaborare per poi scriverli nuovamente all'interno della RAM. Pur essendo molto più veloce degli altri tipi di memoria facenti parte dell'architettura di un computer, è comunque più lenta del processore, e per questo motivo la sua velocità è fondamentale per definire le prestazioni del calcolatore.

Per i motivi sopra descritti tale tipologia di memoria è definita "volatile", poiché non è in grado di conservare i dati contenuti all'interno della stessa una volta tolta l'alimentazione elettrica.

Abstract

Analisi della RAM nella digital forensics

L'analisi della RAM può essere fondamentale nella ricerca di prove nel corso di procedimenti giudiziari; la conoscenza di dati non persistenti e non contenuti all'interno dell'*hard disk* potrebbe essere di fondamentale importanza.
In questo lavoro si sono prima di tutto descritte le due tipologie di salvataggio dati realizzate da un computer.
Esposte inizialmente le modalità di memorizzazione dati all'interno di un computer, sono stati poi descritti i tre metodi utilizzabili per il salvataggio dei dati contenuti all'interno della RAM: *Dump Raw*, *Crash Dump* ed infine *Hibernation File*.
Infine sono stati illustrati i *tool* utilizzabili per l'analisi della RAM, reperibili in commercio, e tramite i quali possono essere raccolte informazioni sulle chat visitate, siti *web* consultati, conversazioni *voip*, e infine ricostruzione di percorsi logici, che non sarebbero individuabili all'interno dell'hard disk, ma che potrebbero essere la chiave di svolta nel corso di una investigazione.

Digital forensics RAM Analysis

RAM analysis could be the key to find evidences in court proceedings; by examining the contents of RAM an investigator can determine a great gain about the state of the machine when the image was collected.
Into this paperwork are described the two computer data storage: live data and memory data.
Once it has been discussed on the three different ways to record RAM data that are called: *Dump Raw*, *Crash dump* and *Hibernation File*, it has been explained how to proceed.
At the end of the paperwork it has been presented the commercial tools actually available on the market and that can be used as valid instruments to extract chat, website and voip information.
Live analysis allow logical path recovery that could not be identifiable using memory analysis and that could be the key point to find evidences.

Francesco Zucconi