Introduzione alla Digital Forensics

I. La Prova Digitale

Tra le varie definizioni di prova digitale adottate a livello internazionale, meritano di essere ricordate quella della International Organization on Computer Evidence (IOCE)[1], secondo la quale la *electronic evidence* «è un'informazione generata, memorizzata e trasmessa attraverso un supporto informatico che può avere valore in tribunale»[2], nonché quella adottata dallo Scientific Working Group on Digital Evidence (SWGDE)[3] per cui costituisce *digital evidence* «qualsiasi informazione, con valore probatorio, che sia o meno memorizzata o trasmessa in un formato digitale»[4].

Stephen Mason[5] osserva correttamente che i termini *electronic evidence* e *digital evidence* sono spesso usati impropriamente come sinonimi, anche se la *digital evidence* costituisce un sottoinsieme della *eletronic evidence*, questa ha una portata definitoria più ampia, comprendente anche tutti i dati in formato analogico (*analogue evidence*). Sono un esempio – tutt'altro che esaustivo – di *digital evidence* le audio e video cassette, le pellicole fotografiche e le telefonate compiute attraverso la rete pubblica: tutte fonti di prova che possono essere "digitalizzate", ma che non nascono in formato digitale.

Sulla base di queste considerazioni, Mason definisce la prova elettronica come «l'insieme di tutti quei dati, inclusi quelli derivanti dalle risultanze registrate da apparati analogici e/o digitali, creati, processati, memorizzati o trasmessi da qualsiasi apparecchio, elaboratore elettronico o sistema elettronico, o comunque disseminati a mezzo di una rete di comunicazione, rilevanti ai fini di un processo decisionale»[6].

A livello legislativo è interessante notare che, su una ricerca effettuata all'interno di 16 Stati europei[7], non è stata rilevata nessuna definizione di prova elettronica e/o digitale. Solo negli ordinamenti di alcuni Stati si riscontrano dei riferimenti alla prova elettronica: secondo il codice di procedura civile finlandese, i supporti cartacei e quelli digitali costituiscono indistintamente «motivi che supportano l'azione»[8]; il già menzionato *Police and Criminal Evidence Act* inglese definisce la prova digitale come «l'insieme di tutte quelle informazioni contenute all'interno di un computer».

I risultati di questa ricerca mostrano, inoltre, come in tutti gli Stati vi sia una sostanziale equiparazione tra documento cartaceo e documento informatico, tra firma autografa e firma digitale e tra posta tradizionale e posta elettronica.

In Italia, l'art. 1, lett. p) del D.lgs. 82/05, anche denominato "codice dell'amministrazione digitale", definisce documento informatico qualsiasi «rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti». Tramite la legge di ratifica della Convenzione di Budapest (legge 48/08), inoltre, è stata abrogata l'aporia normativa esistente nel nostro ordinamento, che vedeva la compresenza, accanto alla definizione appena citata, di quella contenuta nell'art. 491-*bis* c.p. con la quale si intendeva per documento informatico qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria, o programmi specificamente destinati ad elaborarli[9].

Questa nozione faceva riferimento alla materialità del supporto informatico contenente dati o informazioni aventi efficacia probatoria. Oggi, dunque, possiamo definire documento informatico qualsiasi *file* avente un *quid* rappresentativo espresso in linguaggio binario: un testo, un'immagine, un suono e, dunque, anche le pagine dei *social network* o le e-mail.

Paolo Tonini ha evidenziato che la rappresentazione del fatto è la medesima, sia essa incorporata in uno scritto o in un *file*. Quello che cambia è soltanto il metodo di incorporamento su base materiale. Se, ad esempio, il *file* di testo viene stampato su carta, siamo di nuovo dinanzi ad un documento "tradizionale", che esplicita in modo visibile il contenuto del documento informatico. La differenza tra i due concetti (documento tradizionale e documento informatico), dunque, sta tutta nel metodo di incorporamento, e non nel metodo di

---

[1] IOCE è un'organizzazione internazionale costituita nel 1998 con l'obiettivo di creare un luogo di dibattito, di confronto e di scambio di informazioni tra le forze dell'ordine di tutti gli Stati aderenti. Ulteriore obiettivo è quello di redigere delle linee guida per le procedure di acquisizione della prova digitale in grado di garantire che una prova digitale raccolta in uno Stato sia ammissibile anche nello Stato richiedente.

[2] Definizione adottata da IOCE nel 2000: «Electronic evidence is information generated, stored or transmitted using electronic devices that may be relied upon in court».

[3] SWGDE è un'organizzazione internazionale costituita nel 1998, che raccoglie tutte le organizzazioni attivamente coinvolte nel settore della prova digitale e nel settore multimediale al fine di promuovere la cooperazione e di garantire la qualità nel settore della ricerca della prova digitale.

[4] Definizione adottata nel 1999 da SWGDE, all'interno del documento, *Digital Evidence: Standards and Principles*, disponibile al seguente URL: http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm.

[5] Stephen Mason è un avvocato inglese, fondatore della rivista *Digital Evidence and Electronic Segnature Law Review* e membro della IT Law committee of the Council of Bars and Law Societies of Europe.

[6] S. MASON, *Electronic Evidence. Discovery & Admissibility*, LexisNexis Butterwoorths, Londra, 2007, par. 2.03: «Electronic Evidence: data (comprising the output of analogue evidence devices or data in digital format) that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the process of adjudication».

[7] La ricerca è stata effettuata sui seguenti paesi: Austria, Belgio, Danimarca, Finlandia, Francia, Germania, Grecia, Olanda, Irlanda, Italia, Lussemburgo, Portogallo, Romania, Spagna, Svezia e Inghilterra. Per ulteriori informazioni, F. INSA, *The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime-Results of a European Study*, in *Journal of Digital Forensic Practice*, 2006, p. 285.

[8] Legal Proceedings Code of Finland, Chapter 17, Section 11b.

[9] L'attuale formulazione dell'art. 491-*bis* c.p. come modificato dalla legge 48/08 recita: «Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private».

rappresentazione.

I metodi di incorporamento, sempre secondo Tonini, si possono dividere in due categorie fondamentali: quella analogica e quella digitale. L'incorporamento analogico è "materiale", nel senso che la rappresentazione non esiste senza il supporto fisico sul quale è incorporata. Ad esempio, se all'interno di un documento scritto vengono operate delle cancellazioni, resta comunque traccia della manipolazione.

Attraverso il metodo digitale, invece, una rappresentazione è incorporata su di una base «materiale mediante grandezze fisiche variabili»: detto altrimenti, si tratta di una sequenza di *bit*. L'incorporamento digitale ha, dunque, la caratteristica dell'immaterialità, poiché la rappresentazione esiste indifferentemente dal tipo di supporto fisico sul quale il dato informatico è incorporato[10].

Negli Stati Uniti, Eoghan Casey[11] ha definito la prova digitale come «qualsiasi dato digitale che possa stabilire se un crimine è stato commesso o che può fornire un collegamento tra il crimine e chi l'ha commesso»[12].

Nel Regno Unito, Stephen Mason[13] è andato oltre tale definizione, classificando la prova digitale in tre diverse categorie:

– la prova creata dall'uomo: è tale ogni dato digitale che figuri come risultato di un intervento o di un'azione umana che, a sua volta, può essere di due tipi: *human to human* (come ad esempio uno scambio di email), che presuppone un'interazione tra due individui; oppure *human to PC*, come ad esempio la redazione di un documento attraverso un software di videoscrittura. Da un punto di vista probatorio, sarà quindi indispensabile dimostrare che il contenuto del documento non sia stato alterato e che le dichiarazioni in esso contenute possano essere considerate rispondenti al vero;

– la prova creata autonomamente dal computer: ogni dato che figuri come il risultato di un processo effettuato da un software secondo un preciso algoritmo e senza l'intervento umano (esempi possono essere i tabulati telefonici o i *file* di *log*). Da un punto di vista probatorio, in questo caso sarà necessario dimostrare che il software che ha generato questo risultato abbia funzionato correttamente e, ovviamente, che la prova non abbia subito alterazioni dopo che è stata prodotta;

– la prova creata sia dall'essere umano che dal computer: ogni dato che risulta essere il frutto di un contributo umano e di un calcolo generato e memorizzato da un elaboratore elettronico (un esempio può essere un foglio di calcolo elettronico: in esso i dati vengono inseriti dall'essere umano, mentre il risultato viene calcolato dal computer). Da un punto di vista probatorio, sarà necessario dimostrare sia la genuinità dei contenuti immessi dall'essere umano sia il corretto funzionamento dell'elaboratore elettronico.

Se dal 1992, data in cui Collier e Spaul introducono il tema delle modalità di acquisizione della prova digitale come categoria autonoma nella dottrina statunitense[14], la disciplina ha avuto un processo espansivo senza soluzioni di continuità, mai come ora si sente la necessità di un inquadramento normativo.

Di questa esigenza sono matrici concorrenti sia la spinta dell'attualità (si pensi all'emergere delle intercettazioni telematiche) sia lo stesso sviluppo tecnologico, che sta moltiplicando i media e i supporti per convertire le prove, documentali e non solo, in *bit*.

II. La Digital Forensics negli Stati Uniti

La maggior parte delle pubblicazioni scientifiche fino ad ora scritte in materia, hanno utilizzato il termine "computer forensics", espressione coniata nel 1984, quando il *Federal Bureau of Investigation* (FBI) elaborò il progetto *Magnetic Media Program* divenuto, qualche anno più tardi, *Computer Analysis and Response Team* (CART)[15].

A distanza di quasi trent'anni, Ken Zatyko, docente della John Hopkins University, è uno dei primi autori che ha preferito utilizzare il sintagma "digital forensics" in luogo di "computer forensics"[16].

Ritengo più appropriata la scelta del sintagma *digital forensics*, in quanto le analisi forensi sul dato digitale riguarderanno sempre di meno il personal computer e sempre di più altre tipologie di supporti (*smartphone*, lettori mp3, *console* di videogiochi, navigatori satellitari) e di risorse *hardware* o software distribuite in remoto ("cloud computing"), dove sono normalmente archiviati i dati utili ad un'indagine.

Basti pensare che, oggi, uno smartphone è in grado di contenere, molto spesso, le medesime informazioni utili ad un'indagine che potrebbero essere contenute in un personal computer. Ultimamente anche le *console* per videogiochi tendono a somigliare sempre più a computer, con connessioni *wi-fi* e significativi spazi di memoria: aspetti questi, che ne fanno potenziali oggetti di analisi forense[17].

---

[10] P. TONINI, Nuovi profili processuali del documento informatico, in Scienza e processo penale: linee guida per l'acquisizione della prova scientifica, a cura di L. DE CATALDO NEUBURGER, Padova, Cedam, 2010, p. 427.

[11] Eoghan Casey ha conseguito una laurea in Ingegneria Meccanica presso la Berkeley University, e un Master in «Educational Communication and Technology» alla New York University ed è il direttore della rivista «International Journal of Digital Forensics and Incident Response».

[12] E. CASEY, *Digital Evidence and Computer Crime*, Second edition, Elsevier, 2004, p. 12: «*Digital evidence: 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*».

[13] S. MASON, *op. cit.*, par. 2.03.

[14] P.A. COLLIER-B.J. SPAUL, A Forensic Methodology for Countering Computer Crime, in 32 J. For. Sc., 1992, p. 27.

[15] Il progetto CART era costituito da un gruppo di specialisti nell'indagine delle informazioni contenute negli elaboratori. Ulteriori informazioni sul team di lavoro sul progetto CART sono disponibili al seguente URL: http://www2.fbi.gov/hq/lab/org/ cart.htm e all'interno del volume *Handbook of Forensic Services*, 2007, disponibile al seguente URL: http://www.fbi.gov/about-us/lab/handbook-of-forensic-services-pdf.

[16] K. ZATIKO, *Commentary: Defining digital forensics*, in *Forensic Magazine*, 2007, disponibile al seguente URL: http://www.forensicmag.com/node/128.

[17] La particolarità di alcune di queste *console* consiste nel disporre di *avatar* personalizzati, che possono fornire informazioni sulla personalità dei giocatori. In Inghilterra, un uomo ha scoperto che la moglie aveva un amante avendo trovato un nuovo *avatar* tra i giocatori (B. TURNBULL, *Forensic Investigation of the Nintendo Wii: A First Glance*, in *Small Scale Digital Device Forensics Journal*, Vol. 2, No. 1, 2008, disponibile al seguente URL: http://www.ssddfj.org/papers/SSDDFJ_V2_1_Turnbull.pdf). Sempre sul tema è sicuramente interessante il caso che ha riguardato l'attività di *hacking* che ha permesso di conoscere il numero di carta di credito e di altri dati personali di ben 77 milioni proprietari di *consolle Playstation*. Per ulteriori informazioni si veda l'articolo del quotidiano

In quest'ottica, il termine *computer forensics* potrebbe essere riduttivo e non comprendere tutte le categorie in cui viene archiviato il dato digitale.

Eugene Spafford[18], uno dei padri della materia, è il primo a comprendere questo problema e a cercare di darvi una soluzione attraverso la creazione di tre distinte categorie di analisi del dato digitale:

– *computer forensics* in senso stretto (collegata al computer)

– *network forensics* (collegata alla rete)

– *intrusion forensics* (collegata alla violazione di sistemi informatici).

Questa ripartizione, anche se condivisibile, corre il rischio di essere superata dal progresso tecnologico: come già detto, ciò che sta accadendo è la dilatazione della ricerca dei dati dal piccolo bacino del singolo computer all'oceano della Rete (passaggio alla *network forensics*).

Tuttavia, dal momento che la dottrina maggioritaria preferisce utilizzare il termine *computer forensics* anche per l'analisi di dati digitali che a tale categoria non appartengono, nel prosieguo della trattazione verranno indistintamente utilizzati sia il più tradizionale "computer forensics" sia il più generale ed ampio "digital forensics"[19].

Sgombrato il campo da possibili equivoci terminologici, è opportuno ripercorrere le varie definizioni di *digital* e/o *computer forensics* che si sono susseguite negli ultimi anni a livello nazionale e a livello statunitense.

Il *National Institute for Standard and Technology* (NIST) distingue quattro fasi all'interno della *computer forensics*: la raccolta, l'esame, l'analisi, la presentazione, tutte riferite alla prova digitale[20].

La raccolta è data dall'identificazione, etichettatura, registrazione e acquisizione dei dati digitali, nel rispetto di procedure che preservino l'integrità degli stessi.

L'esame consiste nel processo di valutazione del dato digitale attraverso metodi automatizzati e manuali, che preservino l'integrità del dato digitale.

L'analisi, invece, si sostanzia nel processo di verifica dei risultati dell'esame dei dati, al fine di ottenere le risposte ai quesiti per i quali è stato raccolto ed esaminato il dato digitale stesso.

La presentazione dei risultati dell'analisi comprende, infine, la descrizione delle attività compiute e degli strumenti utilizzati, oltre all'eventuale elencazione delle ulteriori operazioni che sarebbero necessarie per completare l'analisi forense.

Nel noto glossario di termini tecnologici (*whatis*) realizzato dal gruppo editoriale on line Techtarget, la *computer forensics* – anche denominata *cyberforensics* – viene definita come l'attività di ricerca e di analisi sulle apparecchiature digitali, finalizzata al reperimento di prove producibili in Tribunale[21].

Questa definizione è analoga a quella proposta durante la Sedona Conference[22] per la quale la *computer forensics* consiste nell'uso di tecniche specialistiche per recuperare, autenticare e studiare dati elettronici, nei casi in cui è necessario effettuare una ricostruzione dell'utilizzo del computer, un esame dei dati cancellati e una certificazione della non alterazione di un dato digitale.

La *computer forensics* richiede competenze specifiche che vanno al di là della mera raccolta e conservazione dei dati effettuata dall'*end-user* pretendendo, generalmente, il massimo rispetto della catena di custodia[23].

Ken Zatyko, definendo la *digital forensics* come «l'applicazione della informatica e delle tecniche investigative in ambito legale», ha distinto otto livelli nel processo di "validazione" della prova digitale:

1. Perquisizione da parte dell'autorità procedente.
2. Rispetto della catena di custodia.
3. Validazione del dato digitale attraverso la funzione di *Hash*.
4. Validazione degli strumenti software utilizzati.
5. Analisi del dato digitale.
6. Ripetibilità.
7. Presentazione dei risultati dell'indagine.
8. Eventuale relazione tecnica da parte di un esperto.

È ovvio che il percorso di validazione della prova indicato da Zatyko impone di avere un consulente tecnico che conosca le dinamiche della *digital forensics* ed è importante che si crei una sinergia tra i legali e gli informatici.

Per Ralph C. Losey[24], il vero protagonista della serie televisiva Star Trek è Scotty, il tecnico che solo raramente appare da protagonista sulla scena, ma assicura la presenza di tutti i dati e di tutti i collegamenti al momento della decisione. Per comprendere l'importanza del "ruolo di Scotty", è possibile portare ad esempio il caso Kevin Keithley v. The Home Store.com[25]. In questo caso, la

on line Guardian, *PlayStation Network hackers access data of 77 million users*, del 26 aprile 2011, disponibile al seguente URL: http://www.guardian.co.uk/technology/2011/apr/26/playstation-network-hackers-data.

[18] B.D. CARRIER-E.H. SPAFFORD, *Categories of digital investigation analysis techniques based on the computer history model*, in *Digital Investigation*, 3, 2006, p. 121.

[19] È interessante osservare che nel contesto statunitense, è spesso utilizzato il termine *e-discovery* per connotare l'analisi forense del dato digitale in ambito civilistico, mentre il termine *computer forensics* ha un'accezione prettamente penalistica.

[20] K. KENT-S. CHEVALIER-T. GRANCE-H. DANG, *Guide to integrating Forensic Techniques into Indente Response*, NIST publication, 2006, disponibile al seguente URL: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

[21] Techtarget, fondato nel 1999 da United Communications Group, è un gruppo editoriale *on line* che tratta il tema della sicurezza informatica. All'interno di tale sito è presente un glossario di grande utilità, disponibile al seguente URL: http://whatis.techtarget.com/ al cui interno è presente la citata definizione di *computer forensics* o *Cyberforensics*, disponibile al seguente URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1007675,00.html.

[22] Il Sedona Conference Institute è costituito da un gruppo di giuristi, avvocati, consulenti tecnici che si confrontano su alcuni temi come antitrust, proprietà intellettuale e *computer forensics*, organizzando conferenze a cadenza trimestrale per permettere agli interessati di ragionare insieme sulle prospettive di sviluppo nelle materie oggetto di studio. Per quanto riguarda la *e-discovery*, uno degli ultimi incontri si è svolto nel gennaio del 2010, il sito di riferimento è disponibile al seguente URL: http://www.thesedonaconference.org/conferences/20100128.

[23] Per una definizione più approfondita della catena di custodia si rimanda ai prossimi capitoli.

[24] R.C. LOSEY, *Introduction to e-Discovery*, ABA Publishing, Chicago, 2009, p. 113.

[25] *Kevin Keithley v. The Home Store.com*, August 12 2008, U.S. Dist. LEXIS 61741, disponibile al seguente URL:

società convenuta aveva realizzato il codice per siti social network molto famosi tra cui anche homebuilder.com o realtor.com ed era stata chiamata in causa per aver violato il brevetto di uno dei loro principali clienti (homestore.com). L'atteggiamento di sufficienza verso la legge aveva portato la società a dichiarare, in accordo con l'avvocato, che tutti i dati relativi al sito social network erano stati cancellati. Questa affermazione convinse il Giudice Laporte a sanzionare il convenuto per distruzione di prove, con una multa di 320.000 dollari, oltre a condannarlo nel merito. Quindici mesi dopo la sentenza di condanna, il nuovo legale, insieme al consulente tecnico, riuscì a produrre alcuni dei codici sorgente che erano stati cancellati e con questa nuova e più collaborativa strategia essi evitarono che il Giudice Laporte ordinasse, oltre alla sentenza di condanna, anche la chiusura della società. Il consulente, quindi, che ritrova il codice sorgente, svolge il ruolo di "Scotty" e riconduce Star Trek su una rotta più sicura.

Tuttavia, questo caso non deve portare a un eccesso di fiducia nell'analisi forense del dato digitale: come osserva correttamente John Patzakis[26], legale della Guidance Software, effettuare una copia forense di un *hard disk* di notevoli dimensioni, per poi andare ad analizzare tutti i singoli *file* cancellati, senza precisi indizi che consentano all'investigatore di escludere buona parte dei risultati, può portare ad una consulenza tecnica particolarmente onerosa e senza alcun risultato concreto.

Patzakis, in altri termini, raccomanda una ricerca di dati che sia il più possibile precisa e limitata, in quanto più la ricerca è vasta, meno è probabile che vengano trovati dati effettivamente utili all'indagine.

Del resto, in ambito civile, gli Stati Uniti hanno adottato, nel 2006, all'interno del Federal Rules of Civil Procedure[27], la regola 26(b)(2)-(B)[28] che circoscrive fortemente l'utilizzabilità delle tecniche invasive per la ricerca di dati inaccessibili[29]. Tale regola prevede che «una parte non è tenuta a fornire la prova di una informazione digitale immagazzinata all'interno di un supporto che essa riconosce come non ragionevolmente accessibile per l'eccessivo volume di dati o per i costi di estrazione […]. La Corte può ugualmente ordinare di fornire tale prova, qualora la parte richiedente dimostri di avere delle valide ragioni, nel rispetto dei limiti previsti dalla regola 26(b)(2)(C)»[30].

Uno dei primi casi dove è stata applicata tale regola (Ameriwood v. Lieberman)[31], riguardava un datore di lavoro che fu autorizzato dalla Corte a realizzare una copia forense dell'*hard disk* di un dipendente, perché aveva fornito alla Corte stessa una "valida ragione" (*good cause*) per effettuare tale copia. La "good cause" si verifica, in particolare, nei casi di sospetta sottrazione di prove, ad esempio quando una parte dichiara che un *hacker* notturno ha cancellato tutti i suoi *file*, o viene misteriosamente smarrito un portatile il giorno prima di un "subpoena duces tecum"[32].

In un altro caso del 2007 (Hedenburg v. Aramark American Food Services)[33], la Corte applicò rigidamente la regola 26(b)(2)(B) e rifiutò l'esecuzione della copia forense del computer di un impiegato, richiesta dal datore di lavoro per farla esaminare da un esperto forense. L'avvocato sostenne piuttosto superficialmente che indagini di quel tipo «erano ormai piuttosto diffuse» e che «di solito, salta fuori qualcosa di nuovo». Il Giudice respinse questo tentativo, che costituiva, secondo lui, una modalità di «andare illegittimamente a caccia di prove». Conviene ribadire che la regola 26(b)(2)(B) si applica a quelle ricerche in cui la "candela del dato" sarebbe di gran lunga inferiore, come resa, alla complessità e al costo del "gioco della ricerca".

Questa interpretazione è, naturalmente, destinata ad evolversi in funzione della tecnologia: la nascita di *hardware* e software sempre più performanti ed efficaci potrà sicuramente modificare la tendenza delle Corti ad interpretare in modo restrittivo la regola.

Rimane il fatto che, nelle Corti civili statunitensi, prove digitali di particolare complessità sono ammesse con riserva al fine di evitare che esse vengano strumentalizzate per paralizzare i processi.

Eoghan Casey, nel 2004, nel tentativo di definire la *computer forensics*, intesa come insieme delle metodologie e delle regole per le investigazioni digitali in ambito penale, distingue, *in primis*, tra il computer utilizzato "come arma" e il computer come "contenitore di dati" relativi alle attività di chi lo utilizza[34].

---

http://ralphlosey.file.wordpress.com/2008/08/keithley. doc.

[26] John Patzakis è stato per molti anni il legale della *Guidance Software* che ha realizzato *Encase* il software di *digital forensics* più utilizzato a livello mondiale: nel 2008, l'80% delle indagini venivano svolte attraverso questo *software*. RALPH C. LOSEY, *op. cit.*, p. 102.

[27] Le *Federal Rules of Civil Procedure* in vigore dal 1938, ma soggette a numerose modifiche nel corso degli anni sono le regole rispettate all'interno dei Tribunali federali dei singoli Stati. In sostanza vi sono due "codici di procedura civile" negli Stati Uniti: quello del singolo Stato e quello federale.

[28] Per una più approfondita analisi della regola 26(b)(2)(B) si veda G.B. MOORE, *Federal Rule of Civil Procedure 26(b)(2)(B) and "Reasonable Accessibility": The Federal Courts'Experience in the Rule's First Year*, in *Privacy & Data Security Law Journal*, disponibile al seguente URL: http://www.bmpllp.com/files/1202334716.pdf.

[29] «Specific Limitations on Electronically Stored Information. A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery».

[30] Rule 26(b)(2)(C): «On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties'resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues».

[31] *Ameriwood Industries, Inc. v. Lieberman et al*., 2007 U.S. Dist. LEXIS 93380, E.D. Mo. Dec. 27, 2006, disponibile al seguente URL: https://ecf.moed.uscourts.gov/documents/opinions/Ameriwood_Industries,_Inc._v._Liberman_et_al-DJS-98.pdf.

[32] Negli Stati Uniti un "subpoena duces tecum" corrisponde a una diffida, soggetta a sanzione se non rispettata, emessa da una Corte. In tale diffida è ordinato a una parte di apparire producendo una determinata prova da usare all'interno di un processo.

[33] *Hedenburg v. Aramark American Food Services*, 2007 US Dist. LEXIS 3443, WD Wash. Jan. 17, 2007.

[34] E. CASEY, *op. cit.*, p. 23.

Nel primo caso siamo in presenza, secondo Casey, di *computer forensics* in senso proprio, mentre nel secondo si assiste a un semplice impatto della dinamica sociale nei sistemi informativi, che non sempre e non dovunque richiede l'utilizzo di tecnologia "forensics" per la ricerca o la conservazione della prova.

Un'ulteriore distinzione molto importante da evidenziare è quella tra *computer forensics* e *computer security*; quest'ultima rappresenta un'area tradizionale della *Information Technology* e si occupa della sicurezza del dato. Tale disciplina in qualche modo interseca il percorso della *computer forensics*, che quel dato vuole acquisire e interpretare.

La differenza fondamentale sta nel fatto che per la *computer forensics* il dato non va solo protetto, ma interpretato e portato in giudizio e l'operatore deve disporre sia di capacità informatiche che di abilità investigative, mentre queste ultime non sono richieste in ambito di *computer security*.

Una data molto importante per l'informatica forense è, naturalmente, l'11 settembre del 2001; da quel giorno la *digital forensics* cessa di essere soltanto uno strumento di indagine e assume anche la veste di strumento utilizzato dalle autorità governative per accedere a tutte le attività che potrebbero potenzialmente essere collegate a iniziative terroristiche.

Questo tipo di utilizzo ha generato una pericolosa, ma in parte inevitabile, tensione tra gli operatori della *digital forensics* da una parte e un fronte esteso di "*antiforensics*" dall'altra, quest'ultimo rappresentato non solo dai difensori della privacy, ma anche dal variegato mondo degli *hacker*.

III. La Digital Forensics in Italia

Anche la dottrina italiana ha avviato un proprio filone di ricerca intorno alla definizione e ai contenuti della *computer forensics*, concentrandosi solo sulla parte relativa ai profili penali delle indagini telematiche. Si tratta di un lavoro ancora embrionale e soprattutto meno suffragato da una giurisprudenza consolidata che, tuttavia, merita il massimo sostegno.

Cesare Maioli definisce la *computer forensics*[35] come «la disciplina che studia l'insieme delle attività rivolte all'analisi e alla soluzione dei casi di criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer, o in cui il computer può rappresentare comunque un elemento di prova». Secondo lo stesso autore, «gli scopi dell'informatica forense sono di conservare identificare acquisire documentare o interpretare i dati presenti in un computer». A livello generale si tratta di individuare le modalità migliori per:

– acquisire le prove senza alterare il sistema informatico in cui si trovano;

– garantire che le prove acquisite su altro supporto siano identiche a quelle originarie;

– analizzare i dati senza alterarli.

Dall'analisi della definizione di Maioli è possibile dedurre alcuni spunti interpretativi:

– i cinque punti cardine della *digital forensic* sono l'identificazione, l'acquisizione, la conservazione, la documentazione e l'interpretazione dei dati;

– il lavoro dell'analista forensics è soprattutto di tipo pratico/informatico.

Similmente, per Marco Mattiucci e Giuseppe Delfinis la 'forensic computing', altro sintagma per indicare la medesima disciplina, si occupa di trattare dati informatici a fini investigativi e/o giudiziari[36]. Il concetto fondamentale cui deve riferirsi la disciplina in esame è quello di "documento informatico", ossia la rappresentazione informatica di atti o fatti giuridicamente rilevanti. Una visione di questo tipo porta gli autori a dare due definizioni della *forensic computing*:

1) «Il processo d'identificazione, conservazione, analisi e presentazione della *digital evidence* (prova legale ottenuta attraverso strumenti digitali);

2) la raccolta e analisi di dati secondo una prassi che ne garantisca la libertà da distorsioni e pregiudizi, cercando di ricostruire dati e azioni, avvenuti nel passato all'interno del sistema informatico».

Ritengo più corretta la seconda definizione, in quanto chiarisce meglio la necessità che durante l'acquisizione del dato digitale non avvengano alterazioni e manipolazioni.

Da ultimo un informatico, Andrea Ghilardini, e un giurista, Gabriele Faggioli[37], definiscono la computer forensics come «la disciplina che si occupa della preservazione, dello studio, delle informazioni contenute nei computer o nei sistemi informativi, al fine di evidenziare prove utili allo svolgimento dell'attività investigativa».

Al di là delle definizioni elencate, la disciplina non potrà essere circoscritta all'aspetto tecnologico, ma dovrà aprirsi alla considerazione di tutti gli aspetti legali interconnessi, come ad esempio:

– il problema dell'aggiornamento delle tecnologie di ricerca, che rischiano di diventare obsolete con conseguente perdita di una grande quantità di dati;

– il problema della "proceduralizzazione certa" nell'acquisizione e nell'utilizzo della prova informatica;

– il problema della privacy e della sua interconnessione (specie dopo l'11 settembre) con l'analisi digitale;

– il problema del rispetto delle norme di legge e più specificamente delle norme processualpenalistiche, la cui violazione ridurrebbe la *digital forensics* a pura interpretazione tecnologica.

Lo studio in campo penale di questa nuova disciplina non può prescindere:

– da un lato, dal tema della congruità dei nuovi mezzi di prova rispetto ai valori fondamentali dell'ordinamento;

– dall'altro, da quello dell'idoneità delle singole attrezzature e dei singoli protocolli applicativi a garantire i diritti della difesa.

---

[35] C. MAIOLI, *Introduzione all'informatica forense*, in *La sicurezza preventiva della comunicazione*, a cura di P. POZZI, Franco Angeli, Torino, 2004, disponibile al seguente URL: http://www.jus.unitn.it/users/dinicola/criminologia/topics/materiale/dispensa_4_1.PDF.

[36] M. MATTIUCCI-G. DELFINIS, *Forensic Computing*, in *Rassegna dell'Arma dei Carabinieri*, 2, 2006, p. 52.

[37] A. GHILARDINI-G. FAGGIOLI, *Computer Forensics*, Apogeo, Milano, 2008, p. 1.