Scienze forensi e tecnologie informatiche: la *computer and network forensics*

GIOVANNI ZICCARDI*

SOMMARIO: *1. Scienze forensi ed evoluzione tecnologica – 2. Alcune definizioni tecniche preliminari – 3. I settori scientifici coinvolti e la multidisciplinarietà della materia – 4. Le quattro fasi d'evoluzione secondo i teorici nordamericani – 5. Lo stato della disciplina: Stati Uniti d'America e Italia a confronto – 6. L'origine della* computer forensics *– 7. Le prime definizioni:* computer forensics, network forensics *e* intrusion forensics *– 8. Il rapporto tra la* computer forensics *e la* computer security *– 9. Eoghan Casey e le definizioni di* computer forensics *– 10. La necessità di un* full spectrum approach *alla* forensics.

1. SCIENZE FORENSI ED EVOLUZIONE TECNOLOGICA

L'origine e lo sviluppo di una disciplina di studio denominata «computer forensics»[1] sono strettamente correlati all'evoluzione dell'*information and communication technology* nell'era moderna[2].

* Professore Associato di Informatica Giuridica e Informatica Giuridica Avanzata, Facoltà di Giurisprudenza, Università degli Studi di Milano.

[1] Ai fini di una preliminare definizione terminologica, si noti che la «s» finale nel termine «forensics» viene solitamente mantenuta nella letteratura anglo-americana (ma non in tutta) perché riferita a «forensics sciences», in cui il termine «sciences» è sottinteso, con il significato di «scienze forensi applicate al mondo del computer». Di qui l'uso del plurale, che può a prima vista apparire inopportuno o non corretto. Nella letteratura italiana, in alcuni casi si predilige il singolare (si veda, *inter alia*, il termine «digital forensic» nel Volume di D. D'AGOSTINI (a cura di), *Diritto penale dell'informatica dai computer crimes alla digital forensics*, Forlì, Experta Edizioni, 2007, oppure in L. CHIRIZZI, *Computer forensic il reperimento della prova informatica*, Roma, Laurus Robuffo, 2006, così come nel titolo del corso di aggiornamento professionale organizzato dall'Università degli Studi di Camerino in, appunto, «computer forensic» o nell'articolo di A. MONTI, *Attendibilità dei sistemi di computer forensic*, in "ICT Lex" 10 febbraio 2003, in Internet all'indirizzo http://www.ictlex.net, sito consultato, e articolo verificato, il 15 marzo 2007). In altri casi si preferisce mantenere il termine al plurale, come da tradizione anglo-americana (si veda, *inter alia*, P. PERRI, *La computer forensics*, in ZICCARDI G., "Manuale Breve di Informatica Giuridica", Milano, Giuffrè, 2006. E. CASEY, studioso di riferimento per queste materie, utilizza preferibilmente le espressioni «forensic science and computer» e «digital evidence». Si è diffusa, in questo settore, anche l'espressione «informatica forense» (cfr. C. MAIOLI, *Introduzione all'informatica forense*, in POZZI P. (a cura), "La sicurezza preventiva dell'informazione e della comunicazione", Milano, Franco Angeli, 2004).

[2] Con riferimento allo stretto rapporto tra evoluzione delle tecnologie ed evoluzione della *computer forensics* cfr. *inter alia* R.G. MASSA, *Le (vere) origini della computer forensics*, in "ComputerLaw

Contestualmente al mutamento portato, in ampi settori della società, dalle nuove tecnologie e, in particolare, dall'avvento dell'elaboratore elettronico e dalle reti, si è verificato un cambiamento nelle modalità di rilevazione, gestione, raccolta e analisi di quegli elementi che, in senso lato e, per ora, assolutamente generico, si possono definire «fonti di prova», «prova», «indizio» o «testimonianza»: si sono affiancati, ad elementi «tradizionali» (naturali e fisici) degli elementi di prova, *lato sensu*, capaci sì di individuare un fatto, ma inscindibilmente correlati ad un elaboratore elettronico o ad una rete informatica o telematica[3].

Il concetto di *computer* forensics (se una particolare attenzione si vuole riservare al computer), di *digital* forensics (se l'attenzione si vuole rivolgere al mondo del dato digitale), di *network* forensics (se l'attenzione si vuole dedicare al mondo delle reti), di *mobile* forensics (se l'attenzione si vuole indirizzare verso i dispositivi mobili), di PDA o SIM *forensics*, ha come elemento essenziale, si è visto, l'idea di *forensics*, ovvero di scienze forensi.

La *computer forensics*, in primo luogo, altro non è che l'estensione di teorie, principi e prassi, proprie della scienza forense in generale, al mondo dell'informatica e delle nuove tecnologie.

Informatica e Diritto", in Internet all'indirizzo http://www.computerlaw.it/entry.asp?entry_ID=200 (sito consultato, e articolo verificato, il 7 settembre 2006) dove si riporta: «quando si parla di computer forensics normalmente ci si riferisce ad una scienza affermatasi con la progressiva evoluzione degli home e personal computers» anche se, sostiene l'Autore, «sebbene la nascita degli hard disk sia datata 1952 (il primo fu un preistorico IBM a 1200 giri al minuto) e l'avvento di altri supporti quali cassette, floppy e cd a momenti successivi, l'analisi, il recupero e la ricostruzione di materiale informatico ai fini investigativi, si spinge fino alla seconda guerra mondiale».

[3] Cfr. *inter alia* L. STILO, *Computer forensics: il volto digitale della scena criminis: necessità di protocolli operativi omogenei*, in "Il Nuovo Diritto", in Internet all'indirizzo http://www.crimine.info/public/crimineinfo/articoli/computer.htm (sito consultato, e articolo verificato, il 7 settembre 2006) secondo cui: «Il processo di neovascolarizzazione informatica ha interessato già da tempo ogni settore dell'attività umana divenendo un aspetto onnipresente nella quotidianità degli ambienti lavorativi e privati. Un esempio per tutti è l'uso dei computer non solo come strumenti di lavoro e svago ma anche come veri e propri mezzi di comunicazione. La diffusione di queste realtà ha fatto aumentare in modo esponenziale le informazioni che vengono create, comunicate ed archiviate in forma digitale. I computer e le altre apparecchiature elettroniche divengono così, sempre con maggiore frequenza, protagonisti e fedeli testimoni del delitto».

Non si tratta, quindi, di un passaggio logico particolarmente complesso, dal punto di vista teorico: la scienza forense (intesa come la scienza che studia il valore processuale di determinati accadimenti ai fini della costituzione di possibili fonti di prova) ha già, in passato, affrontato, senza particolari difficoltà, nuovi «tipi» di prova, nuove metodologie d'analisi, nuovi aspetti delineati dal progresso[4].

Nel caso che interessa in questa sede, si analizzeranno, da un punto di vista informatico-giuridico, le modalità tecniche attraverso le quali la tradizionale scienza forense si è avvicinata al mondo del computer e alle prove (e informazioni) da esso generate: si vedrà che alcuni principi sono rimasti immutati, e hanno potuto risolvere egregiamente problemi anche del «mondo digitale», mentre altri principi si sono dovuti adeguare ai cambiamenti che il computer e l'elettronica hanno inevitabilmente portato.

Nel settore della *computer forensics*, tali cambiamenti hanno riguardato, in estrema sintesi, e ai fini di fornire un quadro «preliminare»:

a) la nascita e sviluppo di una cosiddetta fonte di «prova digitale», che come caratteristiche essenziali ha l'immaterialità e la fragilità intrinseca del dato;

b) lo sviluppo di strumenti (*tools*) di raccolta della fonte di prova digitale, che devono essere utilizzati secondo un certo «metodo», affinché la prima fase di acquisizione della possibile fonte di prova non si riveli inutile o «contestabile» (di qui le costanti affermazioni circa la necessità di linee guida dedicate anche alle metodologie di trattamento della prova digitale);

c) lo sviluppo di nuova tecnologia per memorizzare e far circolare le possibili fonti di prova digitale, per cui ogni giorno il dato che può essere fonte di prova si può trovare memorizzato, o custodito, su un supporto completamente nuovo, e che richiede un trattamento *ad hoc*;

[4] Con riferimento al rapporto tra nuove tecnologie e mezzi di prova si vedano la pregevole Opera di O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico tecnici nuovi o controversi e di elevata specializzazione*, Milano, Giuffrè, 2005 e l'interessante Volume di J. SALLANTIN, J. SZCZECINIARZ, *Il concetto di prova alla luce dell'intelligenza artificiale*, Milano, Giuffrè, 2005, con introduzione di L. LUPÁRIA. Come correttamente ricorda Dominioni, nell'*Introduzione* alla sua Opera, «La cultura della conoscenza giudiziaria ha registrato e, in misura non irrilevante, sta ancora registrando un sensibile ritardo nel farsi carico del rinnovamento delle concezioni epistemologiche in ambito scientifico e tecnologico. Ma ancora maggiore è il ritardo nel mettere a punto i congegni processuali mediante i quali tali concezioni e le nuove risorse scientifico-tecniche di conoscenza siano praticabili nella funzione probatoria con la necessaria affidabilità» (p. 7).

d) il mancato adeguamento a tali cambiamenti da parte di larghissimi settori della società interessati a queste tematiche giuridiche (soprattutto Magistrati, Avvocati, operatori di Polizia Giudiziaria), che si manifesta con una nulla, o lacunosa, preparazione tecnologica (che porta ad ignorare, a volte, lo stesso tema oggetto principale della questione giuridica o a tenere metodi di indagine errati o inefficaci) o alla automatizzazione di deleghe o *expertise* per non analizzare o non occuparsi del problema.

Il primo punto (la nascita di un nuovo tipo di prova, la prova digitale) è un dato incontrovertibile e problematico, in quanto la prova digitale in generale è di difficile identificazione, dal momento che muta costantemente.

In più, il diritto si sta muovendo sempre di più verso la digitalizzazione, nel senso che nella società odierna anche in investigazioni correlate a reati tradizionali vi sono, quasi sempre, aspetti tecnologici[5].

Non appare pertanto peregrina l'affermazione o, meglio, la previsione, che nel prossimo futuro tutta la prova sarà «digitale», in quanto il processo di informatizzazione e digitalizzazione della nostra società condizionerà direttamente, come è ovvio, il mondo giuridico e il suo aspetto processuale[6].

2. Alcune definizioni tecniche preliminari

Prima di riportare definizioni tecniche di eminenti studiosi, sia nazionali sia internazionali, che si sono occupati di queste tematiche, e che con varie modalità cercano di ben inquadrare questa scienza in continua evoluzione, si potrebbe, in assoluta modestia, cercare di dare una definizione di massima, volutamente generica, che possa comprendere ogni possibile aspetto di questa multiforme disciplina.

Una definizione tecnica iniziale potrebbe essere la seguente: per *computer forensics* s'intende quella scienza che studia il *valore* che un dato cor-

[5] Si pensi, a puro titolo di esempio, a: indagini come conseguenza di *crack* finanziari dove sono necessarie operazioni di *forensics* sui computer per recuperare informazioni contabili; analisi del traffico e dei contenuti di *mail* o SMS per questioni di diritto civile (separazioni, divorzi) o penali non strettamente correlate ai reati informatici; questioni di diritto del lavoro correlate alle potenzialità invasive delle nuove tecnologie ai fini del controllo del dipendente.

[6] Con riferimento alle caratteristiche essenziali della prova digitale, agli standard e ai principi, si veda il documento *Digital Evidence: standards and priciples* in *Forensics Science Communications*, April 2000, Vol. 2, No. 2, in Internet all'indirizzo http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm (sito consultato, e documento verificato, il 15 marzo 2007).

relato ad un sistema informatico o telematico può avere in un ambito sociale, giuridico, o legale che dir si voglia[7].

Il concetto di «valore», nel caso *de quo* e dal punto di vista esclusivamente tecnologico, si può intendere come capacità di resistenza ad eventuali contestazioni e capacità di convincimento del giudice e delle parti processuali o di altri soggetti (nel caso si ritenesse che la *forensics* non abbia solo un aspetto strettamente correlato all'ambito *legal*) in ordine alla genuinità, non ripudiabilità, imputabilità e integrità del dato stesso e dei fatti dallo stesso dimostrati.

Come si è ricordato poco sopra, si vorrebbe dare una definizione e un inquadramento innanzitutto tecnologico, lasciando le definizioni giuridiche e processualpenalistiche alle maggiori competenze dell'Autore della Seconda Parte di questo studio; certo è che l'aspetto tecnologico della prova digitale e della *computer forensics* in generale è sempre stato collegato a una

[7] Si vedano, come primo approccio, quattro definizioni tecniche differenti tra loro ma che coprono uno spettro abbastanza ampio in relazione al panorama operativo della *computer forensics*: 1) «Computer Forensics is the use of specialized techniques for recovery, authentication, and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage». (http://www.krollontrack.com/legalresources/glossary.asp, sito consultato, e documento verificato, il 15 marzo 2007); in questa prima definizione l'attenzione è per l'uso di tecniche specialistiche che mirano a recuperare, autenticare o analizzare dati elettronici correlati a comportamenti umani su computer. 2) «The investigation of a computer system or any device that contains a processor and memory in order to determine who, what, where, when and how such digital devices temporary or persistent storage to another device». (http://www.wetstonetech.com/page/page/1972572.htm sito consultato, e documento verificato, il 15 marzo 2007); in questa definizione si vede la *computer forensics* come il metodo per comprendere il chi, cosa, dove, quando e come di un comportamento digitale. 3) «Computer forensics deals with the science of determining computer-related conduct - the who, what, when, where, and how of computer and technology use». (http://www.tecrime.com/gloss.htm sito consultato, e documento verificato, il 15 marzo 2007); simile alla definizione precedente, inquadra la *computer forensics* nella condotta di un soggetto e nei procedimenti investigativi per analizzare ogni aspetto di tale condotta 4) «Computer forensics is the process of investigating data processing equipment – typically a home computer, laptop, server, or office workstation – to determine if the equipment has been used for illegal, unauthorized, or unusual activities. It can also include monitoring a network for the same purpose». (http://en.wikipedia.org/wiki/Computer_forensics sito consultato, e documento verificato, il 15 marzo 2007); quest'ultima definizione unisce alle necessità investigative anche quelle di monitoraggio o controllo dei comportamenti.

«lite», a un processo di contestazione, alla volontà di provare qualcosa in una determinata sede che, nella maggior parte dei casi, è una sede giudiziaria.

Ecco perché, a parere di chi scrive, l'aspetto della «resistenza informatica» alle contestazioni, ovvero la possibilità di provare scientificamente in ogni momento che il dato è integro, non ripudiabile, correlabile direttamente ad un determinato soggetto e che ha valori di luogo e di tempo ben identificabili, diventa l'aspetto centrale in un'analisi definitoria tecnologica della *computer forensics*.

Ad onor del vero, si vedrà ben presto, che la definizione di cui sopra può assumere due aspetti ben distinti nel caso si volesse evidenziare o meno quell'aspetto «sociale» poco sopra evidenziato.

In particolare, avremo una definizione di *computer forensics* «pura», che comprende solo, ed esclusivamente, l'ambito legale, o processuale, dell'acquisizione, analisi e esposizione del dato.

In tal caso, l'aspetto legale è essenziale, e se il dato non «entra» in un contesto giuridico non si può parlare di *forensics*.

Si vedrà, in seguito, che esiste però anche una consolidata tradizione di *forensics aziendale*, una categoria concettuale che può risultare difficile da comprendere se si intende il termine *forensics* correlato esclusivamente all'ambito giuridico.

La *computer forensics* in ambito aziendale altro non è che una *simulazione* di attività che potrebbero essere finalizzate alla produzione della prova in giudizio effettuata, però, in ambito interno aziendale, seguendo, eventualmente, identiche metodologie[8]. Ecco allora che in molte pubblicazioni scientifiche[9] si trova l'accezione *computer forensics* aziendale, o *forensics* aziendale, quando in realtà di *forensics* in senso stretto c'è ben poco.

Ci sono, al contrario, metodologie comunemente utilizzate a fini processuali o da investigatori delle forze di Polizia che vengono usate, in questo caso, per indagini interne aziendali.

[8] Cfr. J.S. RINGOLD III, *Corporate Forensics Toolkit*, in Internet al seguente indirizzo http://mn-isfa.org/presentations/corporateforensicstoolkit.ppt (sito consultato, e documento verificato, il 15 marzo 2007).

[9] Cfr. *inter alia* J. ANASTASI, *The New Forensics: Investigating Corporate Fraud and the Theft of Intellectual Property*, John Wiley & Sons, 2003; C. STEEL, *Windows Forensics: The Field Guide for Corporate Computer Investigations*, Wiley Publishing, 2006.

Si pensi, paradossalmente, ad un'indagine effettuata internamente all'organico di un'azienda da parte di un responsabile del personale usando, in ipotesi, metodologie (interrogatorio, testimonianza) che sono comunemente usate in ambito giudiziario, ma che non hanno alcuna rilevanza esterna al di fuori della struttura aziendale.

Ovviamente, alcune indagini interne di *forensics* aziendale possono, poi, concretizzarsi in azioni esterne, ma ciò non accade sempre.

In questa sede si prediligerà una divisione concettuale delle «due forensics» piuttosto rigida: quando si parla di *computer forensics*, o di prova digitale, o d'indagini, ci si riferisce all'ambito dell'applicazione della legge, strettamente giuridico.

In ogni occasione nella quale si parlerà dell'ambito aziendale, si preciserà che ci si riferisce a *forensics* aziendale (o *corporate forensics*).

I fini delle «due forensics» sono, però, sovente gli stessi: scoprire un determinato fatto, le sue prove, i collegamenti ad uno o più soggetti, valutare se tale fatto è nocivo o meno ed elaborare dei metodi corretti per arrivare a tali fini.

3. I SETTORI SCIENTIFICI COINVOLTI E LA MULTIDISCIPLINARIETÀ DELLA MATERIA

La *computer forensics* è una di quelle discipline dove sono coinvolte competenze difformi tra loro: si può rilevare un aspetto prettamente informatico, uno prettamente giuridico (processuale e tecnico) e uno ì prettamente investigativo.

Non appare, quindi, strano che dette tematiche siano, da tempo, analizzate da informatici, da processualpenalisti, da informatico-giuridici, da Avvocati, da Magistrati, da Forze dell'Ordine, e che ognuno di questi «attori» abbia un approccio singolare e che conduce, sovente, a risultati differenti.

Negli Stati Uniti d'America, visto anche il diverso *curriculum studiorum* tipico delle realtà di matrice anglosassone, si occupano di queste tematiche soggetti che spesso hanno due lauree, una in materie informatiche e una in tematiche giuridiche, o specializzazioni *in utroque*. In Italia la separazione tra giuristi e tecnici è più sentita, con riferimento alla formazione universitaria e post universitaria.

Gli aspetti informatici indispensabili sono essenzialmente correlati alla conoscenza del computer e dei dati, alla comprensione delle procedure e

del *software*, alla capacità di utilizzo pratico degli strumenti più affidabili ed efficaci per effettuare tutte le operazioni necessarie.

Le capacità d'indagine riguardano, invece, il problema di cosa cercare e dove cercarlo, e in caso di presenza di grandi quantità di dati, sono requisiti essenziali per portare a buon fine le attività investigative.

Gli aspetti legali sono anch'essi degni di nota: conoscenze di diritto processuale, soprattutto con riferimento alle corrette modalità di acquisizione della prova (si noti bene: correttezza non solo tecnicologica ma anche legale) devono convivere insieme a conoscenze dei limiti e dei diritti previsti dalla legge, ad aspetti di analisi e profilazione dei comportamenti criminali, di psicologia giudiziaria, di diritto processuale e sostanziale.

Molto spesso le competenze di legali e di informatici si uniscono in maniera cooperativa; in alcuni casi, come nel caso del settore dell'informatica giuridica, si fondono.

Accanto a queste distinzioni preliminari, la *forensics* presenta, poi, un aspetto prettamente teorico congiunto ad un aspetto eminentemente pratico.

Sono numerosi, infatti, gli studiosi che si occupano, nella pratica, di utilizzare gli strumenti per la *forensics*, anche in ausilio alle Forze dell'Ordine o per attività di parte; ma la *forensics* può essere anche attività di studio, di diritto processuale applicato all'informatica, per valutare, ad esempio, l'impatto di dette attività nel sistema del processo.

L'unione di tutti questi aspetti (basi teoriche informatiche e giuridiche, conoscenza della prassi e degli strumenti) contribuisce a disegnare il panorama attuale della *computer and network forensics*.

4. Le quattro fasi d'evoluzione tecnologica secondo i teorici nordamericani

Un eminente studioso di queste tematiche, Eugene H. Spafford, Professore di *Computer Science* presso la *Purdue University*, in una sua premessa ad un testo interessante di *computer forensics* ripercorre l'evoluzione storica di tale materia negli USA: Spafford colloca la nascita della *computer forensics* all'interno della storia delle tecnologie informatiche nell'era moderna[10].

[10] Cfr. G. Mohay, A. Anderson, B. Collie, O. de Vel, R. Mckemmish, *Computer and intrusion forensics*, Boston-London, Artech House, 2003.

In particolare, l'illustre scienziato ricorda, *in primis*, come la *computer science*, o scienza dell'informazione, si presenti come un campo di ricerca relativamente nuovo, non più vecchio di 70 anni; ciò comporta che anche la *computer forensics* in senso stretto si qualifichi come una scienza relativamente recente. Spafford cita, come utile riferimento temporale in questo settore, la più antica associazione di computer, la ACM (*Association for Computing Machinery*), facendola risalire a circa sessanta anni or sono, e il più antico corso di laurea su questi temi, quello della *Purdue University*, che risale a circa quaranta anni or sono.

Ciò dimostra, conclude lo scienziato, che, se comparata ad altre scienze, si è in presenza di una disciplina molto giovane[11].

Nonostante la scienza sia giovane, gli studiosi hanno notato come, in questo pur breve periodo, gli argomenti di attenzione si siano evoluti non poco e siano mutati, sino a dare origine a nuove branche di studio votate ad esplorare nuovi problemi.

La suddivisione in fasi, tanto cara ad un approccio pragmatico come quello d'oltreoceano, viene applicata, dallo studioso statunitense, anche in questo campo.

Spafford, in particolare, identifica quattro fasi di evoluzione, che sintetizza nei modi che seguono.

Si può identificare una prima fase, negli anni Quaranta, dove gli scienziati e gli ingegneri erano impegnati, sostanzialmente, a comprendere e a scoprire che cosa fosse un computer.

Ciò comportava lo sviluppo di nuovi algoritmi, di teorie innovative e di *hardware*; quest'area di studio, come è noto, è ancora attiva e vivace, e comprende anche quella di *debugging*, ovvero di risoluzione dei problemi quando il computer agisce come non ci si aspetta.

La successiva, grande fase dei computer, iniziò negli anni Sessanta con i filoni di ricerca che analizzavano come minimizzare i costi e massimizzare la velocità del computer. Da questo filone hanno avuto origine gli studi sull'affidabilità dell'ingegneria del *software*, sui nuovi linguaggi, sui nuovi sistemi operativi, sullo sviluppo di *hardware* e di reti innovative.

[11] Cfr. G. MOHAY, A. ANDERSON, B. COLLIE, O. DE VEL, R. MCKEMMISH, *Computer and intrusion forensics,* cit.

La terza fase si sviluppò negli anni Ottanta, quando aumentò l'interesse su come rendere i computer robusti e affidabili. In questo caso, ci si cominciò ad occupare della tolleranza del sistema ai guasti e si focalizzò l'attenzione sulla sicurezza: si cominciarono a testare nuovi sistemi per la vulnerabilità e per tenere sotto controllo lo stato della rete.

Negli anni 2000 inizia una nuova fase di interesse per il mondo scientifico, la *computer forensics*, ovvero lo studio di tutti quei fenomeni che dovrebbero aiutare a comprendere cosa succede nel proprio computer e nella propria rete, cercando anche, se del caso, di evidenziare o ricreare dei comportamenti esito di azioni maligne.

Più che esplorare i problemi di sicurezza, o provare l'efficienza dei sistemi, si sviluppano allora strumenti (*tools*) per analizzare, «cristalizzare» e comprendere comportamenti che possano fornire prova diretta o indiretta di un determinato fatto, soprattutto nel caso in cui la prova stessa possa essere distrutta o compromessa da un avversario intelligente e con intenzioni offensive.

Ciò comportò l'origine di un contesto scientifico, e anche pratico, molto differente da quello precedente che comprendeva anche la *computer and network forensics*.

5. Lo stato della disciplina: Stati Uniti d'America e Italia a confronto

L'analisi della *computer forensics* si è sempre basata, anche in Italia, muovendo da parametri «nordamericani»: molti principi, *trend*, situazioni tecniche e giuridiche sono state prese ad esempio e «importate» nel nostro contesto anche quando, in realtà, la situazione legale, soprattutto di base, si presentava molto differente.

L'approccio tecnologico nel mondo nordamericano è ben descritto dallo studioso Casey nell'introduzione alla seconda edizione del suo testo principale, *Digital Evidence and Computer Crime*[12], dove ci si riferisce esplicitamente ad una «esplosione d'interesse nella prova digitale» che si è caratterizzata con discorsi accesi in tema di «strumenti, terminologia, defini-

[12] E. Casey, *Digital Evidence and Computer Crime. Forensic science, computers and the Internet*, Second Edition, Elsevier Academic Press, 2004, p. 1 ss.

zioni, standard, etica». Casey si augura, nell'Introduzione al suo Volume, che l'intero campo di studio possa assumere «maggiore scientificità».

Sono tre, nel pensiero di Casey, i punti che necessiterebbero di approfondimento e di maggiore scientificità nell'analisi; tali argomenti si riportano qui di seguito, al fine di valutare l'impatto che simili distinzioni potrebbero avere anche nel panorama informatico-giuridico italiano.

Il primo punto è la corretta definizione delle aree di specializzazione per chi trova a dover operare nel settore della *computer and network forensics*.

Secondo Casey, non ci sarebbe sufficiente chiarezza, allo stato attuale, sia con riferimento alla individuazione delle aree di specializzazione necessarie, sia a chi dovrebbe ricevere un determinato tipo di «addestramento» o formazione (al profilo soggettivo del *forenser*).

Una prima distinzione di base, che nell'ottica di Casey sarebbe essenziale, è tra «digital crime scene technicians», anche definiti da Casey come «first responders», e «digital evidence examiners». In lingua italiana, i primi si potrebbero definire come tecnici presenti sulla scena del crimine o gruppi di pronto intervento forensi, e i secondi come esaminatori o tecnici di laboratorio. Vi è, quindi, sia una distinzione temporale (riferita al momento in cui i due soggetti dovrebbero intervenire) e una di competenza (i secondi più esperti dei primi).

Nella sistematica dello studioso statunitense questa distinzione sarebbe motivata dal fatto che il *recovery* dei dati richiede molta più conoscenza rispetto alla documentazione, raccolta e preservazione della prova.

A tal fine Casey individua quelle che si potrebbero definire come tre competenze ben specifiche, e nel suo pensiero ben distinte, che richiederebbero diversi livelli di conoscenze e di formazione:

a) *digital crime scene technicians*, che Casey individua come soggetti che, dal momento che avrebbero il compito di assicurare la prova sul luogo del delitto, dovrebbero avere una formazione di base nella gestione della prova e nella sua documentazione così come nella ricostruzione di un crimine, affinché possano localizzare tutte le fonti di prova disponibili con sicurezza, certezza e metodologie corrette;

b) *digital evidence examiners*: questi sarebbero soggetti che hanno competenze documentate e formazione specifica in determinate aree che consentono loro di processare con evidenza e senza errori particolari tipi di prove.

c) *digital investigators*: questi soggetti sono i responsabili, in generale, di tutto il processo di investigazione, e dovrebbero avere, secondo Casey, una formazione generica, di base, completa, ma senz ala necessità, contestualmente, di certificazioni o *training* altamente specialistici. Compito di questi investigatori, secondo Casey, sarebbe anche quello di creare un quadro completo generale, partendo dalle fonti e dai dati trovati dai *first responders*, da presentare in un contesto *legal*.

Un secondo punto critico, secondo Casey[13], riguarderebbe i metodi usati dagli investigatori per assicurare l'affidabilità della prova digitale, e la possibilità che venga a mancare un metodo sistematico che presenti la prova, al termine dell'*iter* investigativo, come affidabile e che corrobori le conclusioni, magari in giudizio, correlate a quella prova.

A tal fine Casey propone, nella sua opera, una vera e propria «certainty scale», scala, o «graduatoria», di certezza riferita ad ogni tipo di prova che aiuti anche a mettere in evidenza le possibili fonti di errore e l'eventuale inaffidabilità intrinseca di un certo tipo di prova.

Il terzo punto di dibattito, secondo Casey essenziale, riguarda la necessità di una standardizzazione. Per Casey, una «crisi» simile a quella che attraversa le modalità di raccolta della prova tradizionali sta attraversando anche il mondo della *digital evidence*, e la mancanza di standard accettati a livello generale sia di pratica sia di *training* si concretizza, in molti casi, in una raccolta delle prove, documentazione e custodia incompleta, e in errori di analisi e di interpretazione della fonte di prova digitale. Secondo Casey, la strada aperta da diverse organizzazioni[14], che consiste nella ricerca di una standardizzazione o di linee guida comunemente accettate, potrebbe essere un buon punto di partenza.

Accanto a questo problema generale, vi è l'«istituto» delle certificazioni, molto comune nella *forensics*, ovvero un sistema che garantisce che un determinato soggetto abbia raggiunto un determinato livello di conoscenza e di pratica.

[13] E. CASEY, *Digital Evidence and Computer Crime. Forensic science, computers and the Internet*, cit., p. 2 ss.

[14] International Organization of Computer Evidence (www.ioce.org), Scientific Working Group on Digital Evidence (www.swgde.org), Digital Forensics Research Work Shop (www.dfrws.org).

Casey vede questo lato formativo e professionalizzante come interessante, anche se ne cita le difficoltà che si sono incontrate, la possibilità di uno standard internazionale di certificazione, che però fatica a muoversi in quanto è difficile conciliare le esigenze di tutti gli attori di questo panorama, soprattutto investigatori, Avvocati, esponenti delle forze di Polizia e magistratura.

In Italia la situazione non è molto dissimile da quella indicata poco sopra da Casey, anche se una definizione precisa di requisiti e qualifiche non si è ancora diffusa.

L'esperienza insegna che gran parte degli esperti di *computer forensics* in Italia, per quanto riguarda l'aspetto delle metodologie informatiche, vanta un *curriculum* tecnico.

La materia ha però trovato ottimi spunti di ricerca anche nell'ambiente giuridico e nel mondo delle professioni legali, grazie all'interesse accademico (soprattutto delle cattedre di informatica giuridica e di diritto processuale penale) e a numerosi Avvocati che hanno iniziato ad analizzare il rapporto che occorre mantenere tra la professione forense e gli esperti informatici chiamati a svolgere perizie o interventi in tema di *computer forensics*, soprattutto in fase di indagini difensive.

L'Università di Camerino ha da tempo attivato (dal 2005) un corso di aggiornamento professionale, in collaborazione con la Polizia Postale e delle Comunicazioni, volto a formare l'esperto in *computer forensic* e a fornire, come si legge nella descrizione del corso, conoscenze tecniche di base necessarie per procedere, durante l'attività investigativa, all'acquisizione di prove informatiche nonché competenze giuridiche atte a valutare il rilievo probatorio dei dati acquisiti. Il corso prevede tre moduli principali: uno riguardante i fondamenti dell'*hardware* e del *software* di un elaboratore elettronico, uno riguardante le discipline giuridico-economiche e uno riguardante la sicurezza e la prova informatica[15].

[15] Il programma del corso, organizzato dalla Facoltà di Scienze e Tecnologie, Corso di laurea in Informatica, in collaborazione con la Polizia Postale e delle comunicazioni, affronta i seguenti argomenti: Modulo 1: Architettura dei Calcolatori Elettronici e loro Programmazione. Architettura dei calcolatori elettronici (evoluzione, elementi funzionali, individuazione degli elementi funzionali all'interno di un calcolatore, reti di calcolatori 20 ore). Programmazione di un calcolatore elettronico (metodologie di programmazione, progettazione del *software*, 10 ore,

Molto interessante, e dedicato agli iscritti alla Facoltà di Giurisprudenza, è il corso di Informatica Forense dell'Università degli Studi di Bologna, tenuto dal Prof. Cesare Maioli, che esamina gli aspetti giuridici e tecnologici attinenti alla prova digitale. In tale corso si analizzano essenzialmente le modalità d'investigazione alla luce dell'ordinamento giuridico italiano: una prima parte del programma riguarda tecniche di indagine scientifica, indagine informatica, investigazione difensiva nel campo dei crimini informatici e dei crimini comuni la cui prova sia costituita da dati digitali o veicolati da sistemi informatici.

Si fornisce poi un quadro dei problemi tecnici, tipicamente informatici, in connessione con le problematiche giuridiche che sottendono a tali tipi d'indagini, soprattutto per quanto riguarda la corretta applicazione del diritto penale e del diritto processuale penale. L'attenzione, come si legge nel programma del corso, si sofferma sull'analisi delle norme rilevanti per le tecniche di acquisizione, conservazione, analisi e produzione dei dati digitali rinvenuti nei computer e dei flussi telematici per la loro utilizzabilità nell'ambito dei vari tipi di processi nonché in altri tipi di istruttoria e procedimento amministrativo sia della Pubblica Amministrazione che delle Autorità indipendenti[16].

il linguaggio Java e suo utilizzo, 20 ore). Principi dei sistemi operativi (10 ore). Modulo 2: Giuridico-Economico. Diritto nella società dell'informazione (normative, crimini informatici, pirateria, sistemi di pagamento, 10 ore). L'amministrazione digitale (codice dell'amministrazione digitale, politiche delle pubbliche amministrazioni, riassetto organizzativo di tipo informatico, 10 ore). *Privacy* e misure di sicurezza (codice della *privacy*, redazione documento programmatico della sicurezza, analisi delle misure minime di sicurezza, 10 ore). I crimini informatici (pirateria informatica, truffe telematiche, violazione dei domicili elettronici e intrusione in banche dati, 10 ore). Profili economici e fiscali del traffico illecito in rete (riciclaggio del denaro sporco, paradisi fiscali, segreto bancario, 10 ore). Modulo 3: Sicurezza e Prova Informatica. La prova informatica (acquisizione della prova, valore della prova nel processo penale, processo civile e processo amministrativo, 10 ore). Laboratorio di *Computer Forensics* (individuazione dei supporti contenenti l'evidenza digitale, criptografia e intercettazioni telematiche, 30 ore). Criptografia (concetti di base, algoritmi di criptografia, criptografia forense, 10 ore). *Hacker* e valutazione di sicurezza dei sistemi (vulnerabilità dei sistemi, sistemi sicuri, *testing* di sicurezza e documentazione, 10 ore).

[16] Il programma dettagliato del corso bolognese riguarda: Parte tecnica: Le caratteristiche fisiche del dato digitale; Tecniche di trattamento del dato digitale a fini processuali: ricerca dei dati, acquisizione, conservazione, analisi, valutazione. Tecnologie relative ai supporti di memorizzazione. Introduzione sulle strutture dei file system più diffusi. Modalità di repertazione

6. L'ORIGINE DELLA *COMPUTER FORENSICS*

La nascita della *computer forensics* si può far risalire, come si è visto poco sopra, ai tardi anni 80 e all'inizio degli anni 90, quando sono stati pubblicati i primi lavori accademici su questi temi.

Si iniziò, in quel periodo, a delineare un nuovo settore che unisce l'informatica al diritto; a margine di questo settore iniziano a sorgere associazioni che si occupano di questi temi, programmi specifici di formazione, organi e corsi di accreditamento e di qualificazione professionale.

La *computer forensics* viene anche studiata, come nuovo settore disciplinare, da tutte quelle «agenzie», negli Stati Uniti d'America, che hanno come compito quello di svolgere indagini e di applicare la legge, sia a livello governativo sia in contatto con le grandi realtà commerciali, bancarie e assicurative.

Contestualmente, con la diffusione su scala mondiale dell'*home computer*, dei telefoni cellulari e dei PDA, si registra un aumento, improvviso e incrementale, del volume di dati che devono essere analizzati e che possono costituire l'elemento centrale per l'individuazione o l'interpretazione di un determinato comportamento criminale o, addirittura, la fonte di prova di un determinato delitto.

Tutto questo materiale, costituito da *file*, *file* di *log* (che tengono traccia delle attività), archivi elettronici, documenti, informazioni temporanee o residuali, o nascoste in aree nascoste non accessibili comunemente nei dispositivi comuni di *storage*, diventa il cuore – il *target*, si direbbe in ambito militare – dell'analisi effettuata dagli esperti di *computer forensics* [17].

di dischi rigidi, di *floppy disk* e di altri supporti. Strumenti *software* di analisi forense. Trattazione di casi pratici su diversi *file system*. Tecniche e strumenti per l'intercettazione di flussi telematici. Parte giuridica: Leggi scientifiche, tecnologia e indagini. Indagini a oggetto informatico. Indagini e trattamento dei dati personali. Le investigazioni difensive in materia informatica. La formazione giuridica del consulente tecnico e del perito in materia informatica. Acquisizione dei dati: strumenti proprietari e open source. La prova digitale in ambito civile. Argomenti collaterali: Le misure tecniche di sicurezza informatica e incident response. La formazione giuridica degli operatori della sicurezza informatica. Cenni di criminologia. Illustrazione di casi.

[17] Cfr. M. G. SOLOMON, D. BARRETT, N. BROOM, *Computer forensics jumpstart*, San Francisco-London, Sybex, 2005.

Una prima definizione, molto chiara e che mette in luce diversi aspetti della *computer forensics*, è quella di C. Maioli, secondo cui l'informatica forense è «la 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»[18] ... e «gli scopi dell'informatica forense sono di conservare, identificare, acquisire, documentare e interpretare i dati presenti su un computer. A livello generale si tratta di individuare le modalità migliori per:

- acquisire le prove senza alterare o modificare il sistema informatico su cui si trovano;
- garantire che le prove acquisite su altro supporto siano identiche a quelle originarie;
- analizzare i dati senza alterarli. In sintesi, di "dare voce alle prove".

L'informatica forense comprende le attività di verifica dei supporti di memorizzazione dei dati e delle componenti informatiche, delle immagini, audio e video generate da computer, dei contenuti di archivi e basi dati e delle azioni svolte nelle reti telematiche»[19].

Analizzando questa definizione preliminare, ma molto completa, di Maioli, si possono ricavare i seguenti spunti interpretativi:

- per lo studioso bolognese l'informatica forense è strettamente connessa all'analisi e alla soluzione di casi legati alla criminalità informatica. Si tratta, quindi, di un'interpretazione molto restrittiva della *computer and network forensics*, che pare escludere tutte quelle operazioni di *forensics* comunque non correlate alla criminalità informatica (ad esempio *forensics* da utilizzare nel processo civile, o in ambito giuslavoristico, o a fini di investigazione interna aziendale). L'approccio è molto simile, in tal caso, a quello di Casey negli Stati Uniti d'America, che unisce la *digital evidence* ai *computer crimes*;
- per Maioli sono essenzialmente cinque i punti cardine della disciplina della *forensics*. Il primo è quello relativo alla conservazione della fonte

[18] Cfr. C. MAIOLI, *Dar voce alle prove: elementi di Informatica forense*, in Internet all'indirizzo http://www.dm.unibo.it/~maioli/docs/fti_informatica_3009.doc.

[19] Cfr. C. MAIOLI, *Dar voce alle prove: elementi di Informatica forense*, cit.

di prova, il secondo quello della identificazione della stessa, il terzo quello della acquisizione, cui seguono le fasi conclusive della documentazione (o reportistica) e interpretazione dei dati;

- gli aspetti eminentemente pratico-informatici, secondo Maioli, sono ben precisi e chiaramente identificabili. Lo scopo dell'analista forense in presenza di dati informatici sarebbe, prima di tutto, quello di adottare metodi di acquisizione della prova che non alterino il sistema informatico oggetto di analisi che contiene le fonti di prova. Occorrerebbe poi garantire un'eguaglianza originale-copia nel caso fosse fatta una copia di un supporto contenente dati per un'analisi in altro tempo o luogo. Infine, la procedura di analisi sulla copia deve comunque avvenire senza causare alterazioni del dato;

- con riferimento ai *target* delle azioni di *computer forensics*, per lo studioso bolognese tali attività devono mirare ai supporti, ai dati generati e ai sistemi, che siano o meno connessi ad una rete, al fine di ricostruire tutte le attività avvenute in un ambiente di *networking*.

7. Le prime definizioni: *computer forensics*, *network forensics* e *intrusion forensics*

Il già citato Spafford, analizzando la realtà informatica e tecnologica moderna, ha proposto una tripartizione del settore della *forensics*, tripartizione abbastanza «rischiosa» in quanto strettamente collegata al tipo di tecnologia: lo studioso statunitense individua infatti una *computer forensics* (correlata al computer), una *network forensics* (correlata alla presenza di una connessione di rete) e una *intrusion forensics* (correlata ad atti di violazione di sistemi informatici). Tale tripartizione è comunemente condivisa, e reperibile anche in altri testi, e si presenta sostanzialmente corretta: l'unico rischio, come accennato poco sopra, è che tale sistema di definizioni possa essere superato dall'evoluzione tecnologica che è in grado di creare nuove categorie (si pensi alla *SIM forensics* che riguarda le procedure di analisi forense sulle SIM dei cellulari).

Di certo, gli anni novanta hanno visto un aumento sensibile della connettività in rete e della presenza di sempre più individui sul *Web*; ciò ha comportato un aumento nella circolazione di messaggi di posta elettronica, di dati, e un aumento correlato e consequenziale di «tracce elettroniche» e della necessità, in taluni casi, di fornire prove di tali comunicazioni.

La conseguenza è stata che l'applicazione di tecniche di investigazione pensate per il mondo tradizionale o per il computer *stand alone* si è estesa al mondo dei *computer network*, che comprende anche le reti *wireless*, le comunicazioni senza fili e i dispositivi portatili.

In pratica, volendo fare un esempio efficace, prima di tale «migrazione» delle attività in rete il «bacino» dove trovare una fonte di prova era limitato ad un insieme di dati contenuti in un computer; con la diffusione della rete, questo bacino è diventato un «mare immenso» che costituisce un luogo ancora più difficile da gestire, in quanto pieno di possibili fonti di prova.

Contestualmente alla diffusione della rete presso il «cittadino comune», dette tecnologie di connessione vengono anche utilizzate dai cosiddetti settori critici della società, ovvero gli uffici governativi, il sociale, il sistema bancario, il sistema medico e di assistenza sanitaria, i punti di distribuzione dell'energia elettrica.

In una società interamente connessa, viene allora naturale pensare a una *network forensics* accanto alla *computer forensics*: la prima ha una connotazione estremamente dinamica (operazioni di indagine su dati che circolano in rete) mentre la seconda ha una valenza più statica (analisi di un computer e dei suoi supporti).

La terza definizione, quella di *intrusion* forensics, ha invece una connotazione più «minacciosa», in quanto starebbe ad indicare qualsiasi attività di indagine effettuata in previsione, o subito dopo, di un *break in* del sistema, di una vera e propria violazione dell'apparato informatico.

Tale partizione della *computer forensics* ha avuto la sua introduzione negli anni Novanta, a causa sia di azioni criminali volte a violare sistemi, sia della diffusione di *virus* e *worm*, ovvero programmi o codici maligni pensati per alterare il funzionamento di computer altrui; una delle parti più interessanti sviluppate da questa «corrente» è sicuramente la reportistica, ovvero studi che vengono pubblicati, diffusi o rilasciati a scadenze temporali definite che analizzano l'azione di *virus*, codici maligni o comandi che mirano ad attaccare sistemi critici per la società tecnologica.

Una data che, certamente, ha modificato sensibilmente le prospettive di chiunque si occupi di sicurezza, e che ha influito anche sullo sviluppo della *computer forensics*, è l'11 settembre 2001, ed i motivi sono diversi.

In primo luogo non va dimenticato che la *computer forensics* è essenzialmente uno strumento, seppur tecnico, d'indagine.

Dopo l'11 settembre, come conseguenza di una maggiore richiesta d'indagini da parte degli enti governativi, la *computer forensics* ha assunto anche la «pericolosa» forma di possibile strumento in grado di fornire alle autorità governative un accesso quasi senza limiti alle informazioni che potrebbero essere rilevanti nella investigazione di sospette attività terroristiche.

Vista la premessa indicata poco sopra (ovvero che oggi la maggior parte della società è connessa, ovvero collegata a reti di informazioni), la conclusione immediatamente successiva è che la *computer forensics* potrebbe essere la «leva» per avere accesso senza alcun limite a tutte le informazioni che circolano in un determinato contesto sociale.

Di particolare interesse, su tale punto, e strettamente collegato all'aspetto di cui sopra, è stato lo sviluppo della cosiddetta *anti-forensics*, ovvero di strumenti e tecnologie che permettano di evitare, eludere o ingannare i controlli e le indagini effettuate con i tipici metodi della *computer forensics*.

Si pensi alla *anti-forensics*, in questo caso, come ad un mezzo per garantire la propria *privacy* nei confronti di un *misuse* o *abuse* delle tecniche di indagine o, al contrario, in un'ottica prettamente criminale, all'uso dell'*anti-forensics* per evitare di lasciare tracce dell'attività criminale o per presentare risultanze capaci di ingannare gli investigatori.

8. Il rapporto tra la *computer forensics* e la *computer security*

Nel settore dell'*information technology* vi è un'area disciplinare, quella della sicurezza informatica, o *computer security*, che vanta una tradizione ben più risalente della *computer forensics*: già dall'apparire dei primi elaboratori elettronici, a fianco delle problematiche sulla comprensione del loro funzionamento, si posero i primi problemi sulla sicurezza di detti sistemi.

Non bisogna quindi stupirsi se una parte della dottrina, visto che la *computer forensics*, pur dalla prospettiva delle indagini, incontra problemi di sicurezza informatica, ha iniziato a discutere del rapporto tra *computer security* e *computer forensics*. Tale discussione, a parere di chi scrive, non ha grande interesse né scientifico né definitorio, ma può fornire buoni spunti per proseguire in un'analisi metodica di questa disciplina.

Da un certo punto di vista, si potrebbe evidenziare un certo distacco tra l'esperto di *computer forensics* e l'esperto di *security*, soprattutto se si volessero individuare le competenze del primo in un *mix* tra conoscenze tecnologiche e *skill* investigativi.

Si veda, a tal proposito, una definizione contenuta nel *The New Shorter Oxford English Dictionary*, citata in numerose occasioni, per cui la differenza sarebbe che nell'ambito della forensics vi è «l'applicazione delle scienze forensi e delle tecniche correlate a materiale basato su computer. In altre parole, è il processo di identificare, preservare, analizzare e presentare la prova digitale in un modo che sia accettabile in un procedimento legale o in un contesto legale».

Rispetto alla *security* in generale, quindi, la *computer forensics* comprenderebbe, in più, un'analisi critica del dato informatico (ad esempio dopo un'intrusione) ma che è mirata a una cosiddetta *electronic discovery*, ovvero alla produzione di documenti utili per eventuali contestazioni o per essere portati in giudizio.

Per concludere il discorso, certamente i due settori vantano competenze necessarie, e tecniche applicate, che si sovrappongono.

Il procedimento di base, ad esempio, è un chiaro caso di *overlapping*: le competenze che servono per conoscere a fondo un computer e saper dove cercare i dati, sono tipici sia dell'esperto di *computer security* sia di quello di *forensics*.

La *forensics* ha però alcune caratteristiche particolari che sono tipiche, e che si discostano dall'idea di *computer security* tradizionale; tali aspetti si potrebbero individuare in:

- l'identificazione della prova, ovvero la comprensione – quasi la «premonizione» – di dove si possano cercare quei dati che potrebbero essere usati come fonte di prova;

- la determinazione chiara su come preservare la prova. Molti interventi di *security* sono istantanei; nel caso della *forensics* occorre anche programmare la conservazione, magari per lungo tempo, del dato digitale al fine di presentarlo eventualmente in un ambiente dove sarà discusso, analizzato e, presumibilmente, contestato;

- il processare e interpretare la prova non secondo «standard informatici» bensì inquadrandola come strettamente collegata a fatti naturali che costituiscono la base di una questione che viene discussa, sia essa un crimine contestato o una causa civile;

- assicurarsi che tutte le operazioni informatiche fatte sul dato digitale siano accettabili – nelle pagine precedenti abbiamo usato il termine «resistenti» – in un contesto giuridico.

A parere di chi scrive, la differenza sostanziale tra la *computer security* e la *computer forensics* non risiede tanto nei metodi utilizzati o nelle tecniche da apprendere (molti esperti di *computer security* sono anche degli esperti *forenser*, e molti esperti di *computer forensics* vantano certificazioni o *training* specifico in tema di *security*, di *intrusion detection* e di *incident response*) ma nei presupposti in base ai quali si tratta il dato digitale.

Se al centro dell'attenzione c'è la sicurezza del sistema e il suo buon funzionamento (compresa la predisposizione di adeguati mezzi affinché il sistema non possa essere violato) ci si trova nel campo della *security*; se al centro c'è un ambiente legale dove si deve portare il dato, per varie finalità e, quindi, ogni azione deve avere come metodo e come presupposto la consapevolezza che il dato raccolto è destinato ad un contesto non informatico ma giuridico, allora si è in presenza della *computer forensics*.

9. EOGHAN CASEY E LE DEFINIZIONI DI *COMPUTER FORENSICS*

In un articolo che apre il primo numero della Rivista scientifica *Digital Investigation*, Eoghan Casey[20], illustrando gli scopi e gli argomenti della pubblicazione in oggetto, si sofferma sul problema definitorio della scienza di cui ci si occupa.

In primis, Casey separa nettamente due situazioni che, nel suo pensiero, sono ben distinte:

1) i computer come «arma» utilizzata dai criminali moderni (si pensi a un furto perpetrato tramite computer, a reati sessuali contro bambini, all'uso delle tecnologie più avanzate nel mondo del traffico di droga e del crimine organizzato, all'uso di prove digitali nel caso di contestazioni di diritto del lavoro o civili);

2) il caso, invece, in cui i computer non siano direttamente coinvolti nella commissione di un crimine, ma contengano dati che riflettono le attività di chi li usa. Come è noto, infatti, i dati presenti su personal computer, nei telefoni cellulari, su *device* mobili, su reti possono stabilire con precisione notevole quando è avvenuto un fatto, dove si trovavano le vittime e i sospetti, con chi hanno comunicato, e così via.

[20] E. CASEY, *The need for knowledge sharing and standardization*, in *Digital Investigation* (2004), 1, p. 1-2.

La conclusione di questa prima suddivisione, per Casey, è che molto spesso un'attività di investigazione «tradizionale» viene a toccare anche il mondo dell'informatica e dei computer, seguendo il filo logico che abbiamo già illustrato nel primo Capitolo per cui se la società si muove verso la tecnologia, anche ogni questione giuridica (dato che il diritto è lo «specchio» della società) avrà una connotazione informatica o telematica.

Secondo Casey, questo cambiamento nel panorama «sociale» e giuridico ha condotto a un problema definitorio, sino a creare confusione nelle definizioni e nella terminologia fondamentale.

Come prima cosa, Casey ha notato, nel suo scritto, che molti professionisti della sicurezza e molti soggetti che operano in ambito militare, utilizzano i termini «computer forensics» o «digital forensics» per riferirsi a tutti gli aspetti d'investigazione in caso di un attacco o di una violazione della sicurezza, mentre nell'ambito del *law enforcement*, nota Casey, tali termini si applicano solo quando devono essere utilizzate delle procedure di gestione della prova corrette.

A complicare il quadro, vi sarebbe poi un disaccordo, secondo Casey, con riferimento al ruolo dei *log* dei *server*, del traffico di rete e degli altri dati presenti in Internet, che portano alla diffusione di termini quali *network forensics* e *incident forensics*.

10. La necessità di un *full spectrum approach* alla *forensics*.

In un recente studio del *First Digital Forensic Research Workshop* che si è tenuto al *Rome Research Site* dell'*Air Force Research Laboratory*[21] si è evidenziato come la *forensics* del futuro non riguarderà solo gli aspetti tecnici.

Focalizzarsi solo sull'aspetto tecnologico, secondo i redattori di questo studio, rappresenta un approccio assai limitativo per risolvere i problemi posti da questo delicato settore di ricerca: appare indispensabile, infatti, mantenere una costante attenzione anche alle procedure e agli aspetti legali.

Questo *full spectrum approach* alla *forensics*, sicuramente molto interessante, riguarda quattro aspetti essenziali:

1) un aspetto prettamente tecnico. Il primo problema da risolvere, da un punto di vista tecnico, è quello dell'aggiornamento, in quanto la tec-

[20] In Internet all'indirizzo http://www.if.afrl.af.mil/.

nologia muta rapidamente, aumentano le dimensioni dei sistemi di *storage* e, quindi, di potenziale materiale da investigare, e i tools di analisi diventano spesso obsoleti o non sono in grado di gestire grandi quantità di dati.

2) Un aspetto prettamente procedurale. L'analisi forense deve raccogliere tutto il materiale che potenzialmente possa contenere fonti di prova, e ciò vuol dire analizzare e vagliare tantissime informazioni a supporto delle investigazioni. Il problema, da un punto di vista squisitamente procedurale, è che sovente non esistono procedure, linee guida, protocolli standard o, se esistono, non vengono molto spesso applicati, conosciuti o standardizzati. Si pensi, come notano in molti, che a volte non sono neppure usate terminologie standard per indicare gli stessi fenomeni.

3) Un aspetto prettamente sociale. Le attività di *forensics*, come si è visto poco sopra quando si parlava del *post* 11 settembre 2001, pongono seri problemi sociali, soprattutto con riferimento alla *privacy* dell'individuo e alla raccolta e all'analisi dei suoi dati. Qui il problema centrale è che molto spesso le esigenze degli investigatori spesso entrano in collisione con i diritti del soggetto sottoposto ad indagine: si pensi all'annoso dibattito sulla custodia dei *file* di *log* e delle tracce delle comunicazioni, custodia che si richiede la più lunga possibile da parte degli investigatori, e la più breve possibile da parte dei soggetti intercettati, osservati o «loggati».

4) un aspetto prettamente legale, o giuridico che dir si voglia. Si possono utilizzare le tecnologie più avanzate esistenti, le tecniche più sofisticate, i sistemi più sperimentali sul mercato, ma se l'attività di indagine forense sui dati informatici non è conforme alle regole, soprattutto procedurali, dettate dalla legge, tutto ciò è assolutamente inutile.

A parere di chi scrive, questo approccio «quadripartito» è davvero interessante e denso di spunti e stimoli di ricerca; soprattutto, è un approccio che non si focalizza sugli aspetti tecnici della *forensics* ma che ne analizza anche gli aspetti sociali e giuridici che, a volte (soprattutto in ambiente tecnico e informatico) vengono considerati di marginale importanza.