Evidenza informatica, computer forensics e best practices

Maurizio Tonellotto[•]

Riassunto
La prova informatica negli ultimi anni ha assunto un ruolo sempre più rilevante non solo nell'ambito delle indagini digitali ma, più in generale, nella quasi totalità delle attività investigative, andando spesso a rivestire l'ingrato compito di prova principe nei vari procedimenti.
Nell'articolo verranno evidenziate le peculiarità di questo nuovo elemento probatorio e saranno passati in rassegna i principali strumenti giuridici, anche in relazione alla recente ratifica della Convenzione di Budapest sui computer crimes,. Inoltre, saranno esaminati alcuni aspetti relativi ai protocolli operativi o alle best practices in uso a livello internazionale in un'ottica comparativa con la realtà nazionale.

Résumé
La preuve informatique a joué un rôle de plus en plus important au cours des dernières années, non seulement dans le domaine des investigations numériques mais, plus généralement, dans presque toutes les activités d'enquête, ayant souvent la tâche ingrate de preuve principale dans les différentes procédures judiciaires.
L'auteur met brièvement en évidence les caractéristiques de cette nouvelle preuve, énumère les instruments juridiques, y compris la récente ratification de la Convention de Budapest sur la cybercriminalité et analyse les protocoles opérationnels et les bonnes pratiques au niveau international, dans une perspective comparative avec la réalité nationale.

Abstract
Digital evidence has taken an increasing role in recent years not only in the field of digital investigation but, more generally, in almost all investigative activities. It often plays the unpleasant role of main evidence in the judicial proceeding.
This article will highlight the particularities of this new kind of evidence and review the main legal instruments related, not only but also, to the recent ratification by Italy of Budapest Convention on Cybercrime. It will also examine some aspects of operational protocols and best practices at international levels in a comparative perspective with Italian context.

[•] Dottorando di Ricerca in Sociologia e Ricerca Sociale, settore di ricerca Criminologia (SPS/12), presso il Dipartimento di Sociologia e Diritto dell'Economia dell'Università di Bologna. Sovrintendente della Polizia di Stato in servizio presso il Compartimento Polizia delle Comunicazioni di Bologna, analista forense e consulente tecnico per numerose Procure della Repubblica tra cui Bologna, Ferrara e Forlì.

1. Alcune definizioni preliminari.

La *computer forensics*[1] difficilmente trova una definizione univoca ed esaustiva che la possa descrivere in modo corretto in tutte le sue sfumature[2].

In via generale per *computer forensics* si potrebbe indicare quell'attività tecnico-investigativa finalizzata all'individuazione, acquisizione, preservazione, gestione, analisi ed interpretazione di tracce digitali, rinvenibili all'interno di elaboratori o dispositivi elettronici, nonché la loro correlazione ai fatti, alle circostanze, alle ipotesi ed alle tracce di qualsiasi natura, rinvenute o comunque afferenti al fatto investigato.

Corre l'obbligo dunque, in questo saggio, di esaminare alcuni elementi definitori presenti nella dottrina preminente, al fine di fornire un quadro d'insieme quanto più possibile organico.

Per buona parte della letteratura la *computer forensics* rientra a pieno titolo nel novero delle dottrine della criminalistica, intesa come l'applicazione delle metodologie scientifiche funzionali all'investigazione criminale[3].

In base a tali interpretazioni la *computer forensics*, che nella sua accezione più generalista viene indicata anche *digital forensics*, potrebbe essere intesa, e forse erroneamente confusa, come attività esclusiva di polizia scientifica alla stregua della balistica, della dattiloscopia, della medicina legale, ecc. [4].

In una recente opera viene infatti precisato come "[…]*si ha a che fare, senza dubbio, con una nuova specializzazione dell'attività di polizia scientifica – al pari della balistica, della genetica, dell'entomologia applicate – che entra in gioco nel momento in cui le evidenze dell'azione criminosa sono reperibili 'nel mondo digitale'*"[5].

In questo contesto l'attività di *computer forensics* sarebbe strettamente correlata alla scena del crimine ed agli elementi che da essa scaturiscono.

In un saggio apparso su *Ciberspazio e Diritto* nel 2010 un altro autore evidenzia come "*La computer forensics è un processo teso alla 'manipolazione controllata' e più in generale al trattamento di dati e/o informazioni digitali e/o*

[1] Al fine di un chiarimento terminologico per il presente articolo, si vuole sottolineare la scelta dell'uso della "s" finale nel termine "*forensics"* che in prima battuta potrebbe apparire non corretto o inopportuno. Tale connotazione viene solitamente mantenuta in buona parte della letteratura anglo-americana in quanto direttamente riferibile al concetto di "*forensics sciences"* e dunque scienze forensi. Nel panorama italiano la letteratura evidenzia come taluni autori prediligano l'utilizzo del singolare ed altri la terminologia americana classica, come si è scelto di adottare in questa sede. Per un'analisi puntuale sull'utilizzo di tale terminologia si rimanda a G. Ziccardi, "Scienze Forensi e tecnologie informatiche", L. Luparia, G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007, p.3.

[2] Per un approfondimento puntuale sull'argomento si rimanda *inter alia* a: E. Casey, *Digital Evidence and Computer Crime Forensic Science, Computers, and the Internet*, Academic Press, Londra 2000; J. Henseler, "Computer Crime and Computer forensics", *Encyclopedia of Forensic Science*, Academic Press, Londra, 2000; L. Luparia, G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007; L. Luparia (a cura di), *Sistema penale e criminalità informatica*, Giufrè, Milano, 2009.

[3] A riguardo si consideri, *inter alia*, A. Ghirardini, G. Faggioli, *Computer forensics*, Apogeo, Milano, 2007 ed anche S. Aterno, F. Cajani, G. Costabile, M. Mattiucci, G. Mazzaraco, *Computer forensics e Indagini Digitali, Manuale tecnico giuridico e casi pratici*, Forlì, Experta, 2011.

[4] Nella sua accezione più ampia la *Computer Forensics* viene proposta anche con il termine *Digital Forensics*, indicando con questo il complesso delle indagini e l'analisi delle tracce digitali rinvenute e repertate non esclusivamente all'interno di elaboratori elettronici, ma anche all'interno di tutti quei dispositivi digitali che hanno capacità di memorizzare informazioni e/o dati (telefoni cellulari, *tablet*, *computer* palmari, sistemi di navigazione satellitare etc.).

[5] A. Ghirardini, G. Faggioli, *op. cit.*, p.1.

sistemi informativi per finalità investigative e di giustizia"[6].

L'esplicito riferimento alla "*manipolazione* […] e *trattamento di dati"* pone tale disciplina in relazione all'attività logico inferenziale tipica, appunto, della ricerca scientifica ed anche dell'analisi forense.

La cosa certa è che l'origine e l'evoluzione della *computer forensics* siano strettamente legate al progresso dell'*information and communication technology*.

E' infatti proprio lo sviluppo delle nuove tecnologie ed in particolare delle reti di comunicazione, della diffusione massiccia di elaboratori elettronici e dei sistemi informativi distribuiti, che porta ad un mutamento delle modalità di rilevazione, raccolta, gestione ed analisi di elementi che, in ambito processuale, potrebbero essere definiti come indizi, prove o fonti di prova, ovvero tracce digitali, impalpabili ed estremamente volatili, che si affiancano e talvolta sovrastano quelle di tipo tradizionale.

Un'ulteriore e puntuale definizione viene proposta da Maioli, il quale indica come l'informatica forense sia "*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"*[7]. Lo studioso bolognese, nel fornire tale definizione, delinea maggiormente il contesto più propriamente investigativo della *computer forensics* anche se, nell'economia del suo discorso, viene limitato ai soli reati informatici.

Tuttavia l'affermazione non può essere generalizzata poiché relegare l'informatica forense alle sole indagini digitali concernenti i reati informatici[8], così come definiti nei dettami del diritto sostanziale, può apparire riduttivo anche alla luce delle prassi investigative messe in risalto da noti episodi di cronaca, concernenti ipotesi di omicidio, che hanno visto proprio l'analisi delle tracce informatiche come elemento fondante di tesi accusatorie da una parte e come supporto all'azione difensiva dall'altra[9].

Pare opportuno pertanto, in via preliminare, allargare il quadro definitorio, analizzando alcune apparenti ambiguità che potrebbero, non correttamente, limitarne lo studio ai soli aspetti tecnici.

E' infatti necessario un approccio interdisciplinare all'argomento in discussione che, pur mantenendo un valore epistemologico, sposterebbe l'attenzione su valutazioni di natura differente.

In quest'ottica si potrebbe indicare come la "*computer forensics sia quella disciplina che studia il valore che un dato correlato ad un sistema informatico o telematico può avere in qualunque ambito sociale. Tale valore deve essere inteso come la capacità del dato di resistere alle contestazioni influenzando il libero convincimento*

[6] G. Costabile, "Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008", in *Ciberspazio e Diritto*, n. 3, 2010, p. 465.

[7] 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 (sito consultato e documento verificato, in ultimo, in data 13/12/2013).

[8] A tale riguardo si ricordano le fattispecie delittuose novellate dalla legge 547/93 e le sue successive modifiche non da ultimo la L.48/2008.

[9] Ci si riferisce, ad esempio, alle indagini relative all'omicidio di Chiara Poggi, all'omicidio di matrice terroristica del Prof. Marco Biagi o, anche, ai fatti di cronaca legati all'omicidio di Meredith Kercher, dove le evidenze informatiche hanno assunto un ruolo estremamente importante durante le fasi processuali.

del giudice in ordine alla genuinità, non ripudiabilità, imputabilità ed integrità del dato stesso e dei fatti dallo stesso dimostrati"[10].

La definizione proposta da Ziccardi puntualizza in primo luogo la fondamentale importanza che riveste il dato digitale e come questo debba essere obligatoriamente correlato con altri elementi affini.

Spingendosi oltre l'orientamento dello studioso appena menzionato, potremmo concludere indicando come sia di primaria importanza la correlazione del dato, nella sua accezione più generale e dunque inteso non esclusivamente digitale, con altri elementi acquisiti nel corso delle indagini.

Oltreoceano Rosen indica la *computer forensics* come l'applicazione della *computer science* al processo investigativo[11], Judd Robbins ne parla come l'applicazione delle investigazioni su *computer* delle tecniche di analisi in modo da determinare potenziali prove aventi valore legale[12].

Taluni ancora la vedono come l'utilizzo di *computer*, anche connessi in rete, per risolvere casi giudiziari tramite attività volte all'analisi e soluzione di ipotesi collegate alla criminalità informatica[13].

Infine la recente pubblicazione dello standard ISO/IEC 27037, pur non fornendo una indicazione puntuale di *computer forensics*, si sofferma sul concetto di *digital evidence*, definendola come ogni informazione che può essere memorizzata o trasmessa in forma digitale che è o può essere considerata evidenza[14].

In questo caso dunque elemento centrale è il dato digitale, che può assumere rango di prova a prescindere dagli ambiti investigati.

E' indiscutibile comunque come lo scopo dell'informatica forense sia quello di individuare, identificare, acquisire, documentare e, di certo in maniera assolutamente prioritaria, *interpretare* i dati presenti su *computer*, ovvero all'interno di dispositivi elettronici o ad alto impatto tecnologico.

Tale *interpretazione* del *dato*, lungi dall'essere una sterile disamina sistematica di tipo meramente ingegneristico ed automatizzato, deve poter tener conto del contesto investigato, degli indizi acquisiti, degli elementi e delle ipotesi formulate nel corso delle indagini.

Solo una correlazione di più elementi, non per forza di natura esclusivamente digitale, permette di contestualizzare l'evidenza informatica, facendole assumere il ruolo ben più importante di fonte di prova.

---

[10] G. Ziccardi, *Scienze Forensi e tecnologie informatiche, cit.*, pp. 10-11.

[11] R. A. Rosen, *Forensics e frodi aziendali, intervento alla Giornata di studio A.I.E.A.*, Roma, 21 novembre 2001.

[12] "*Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud*", in J. Robbins, *An explanation of computer forensics*, in internet all'indirizzo http://www.pivx.com/forensics (sito consultato e documento verificato, in ultimo, in data 13 dicembre 2013).

[13] D. Forte, "Le attività informatiche a supporto delle indagini giudiziarie", in *Rivista della Guardia di Finanza*, 2, 2000, p. 543.

[14] ISO/IEC 27037, *Guidelines for identification, collection an/or acquisition and preservation of digital evidence*, approvato e pubblicato in ottobre 2012. Il testo nella sua versione inglese riporta al paragrafo 3.5 "*digital evidence: information or data, stored or*

2. Multidisciplinarità della computer forensics: computer forensics, digital investigation e criminalistica.

Nell'ambito delle indagini giudiziarie, al fine di poter addivenire ad un quadro probatorio certo oltre ogni ragionevole dubbio, le prove indiziarie rinvenute sulla *scena crimins* dovranno necessariamente essere messe in relazione con altri elementi.

Per fornire una valenza probatoria, dunque, anche le ipotesi ottenute a seguito dell'analisi delle singole tracce informatiche dovranno trovare conferma attraverso un procedimento inferenziale di correlazione tra più fonti.

Tale procedimento di astrazione viene tipizzato nell'attività di indagine di Polizia Giudiziaria, ovvero in un'azione investigativa coordinata.

In linea di principio, si deve considerare come le tracce rilevate su un elaboratore non possano sempre risultare esaustive o sufficienti a delineare gli elementi probatori per una condotta delittuosa.

Basti pensare che con le necessarie competenze tecniche sulla rete Internet non è di fatto impossibile compiere una qualsiasi azione nel più completo e totale anonimato, ed è altrettanto vero però che una qualsiasi operazione nel mondo virtuale lascia, come nel mondo reale, delle tracce, deboli, a volte precarie e non direttamente rilevabili, che in linea di massima possono essere utilizzate per ricostruire l'azione, al fine di individuare l'elaboratore attraverso il quale sia stata posta in essere una determinata condotta.

Pertanto, anche in considerazione delle peculiarità dell'evidenza digitale, appare indubbio come la *computer forensics* non possa essere relegata ad una mera attività tecnica e funzionale alle investigazioni poiché la necessità di correlare molteplici elementi, al fine di addivenire a risultati quanto più prossimi alla realtà investigata, comporta inevitabilmente un procedimento di astrazione e deduzione inferenziale, molto più vicino all'attività investigativa che a quella tecnico scientifica. La *computer forensics* dunque dovrebbe, più correttamente, trovare la sua collocazione proprio nell'ambito delle indagini criminali e non essere confinata alle sole attività di polizia scientifica.

Sulla base di quanto asserito ed al fine di sgomberare il campo da alcune ambiguità semantiche che potrebbero adulterarne un approccio quanto più corretto, sarebbe opportuno riferisi a tale disciplina con un'accezione più ampia quale quella di *digital forensics investigation* che, racchiudendo in sé i concetti di investigazione e di scienze forensi, ne fornirebbe una sua migliore collocazione nel contesto tecnico-investigativo[15].

Quanto detto sopra non è da considerarsi esclusivamente come un mero esercizio stilistico o accademico con lo scopo di fornire una definizione di tale disciplina, bensì trova giustificazione nel fatto che, com'è noto, la criminalistica, come tutte le attività di polizia scientifica, affianca le indagini fornendo elementi indiziari e giustificazioni scientifiche alle ipotesi

transmitted in binary form that may be relied on as evidence".

[15] Per un approfondimento sull'approccio investigativo al concetto di *digital forensics* si rimanda, *inter alia*, ad A. Agarwal *et al.*, "Systematic digital forensic investigation model", in *International Journal of Computer Science and Security (IJCSS)*, vol. 5,1 2011, p. 118-131; S. Alharbi, J. Weber-Jahnke, I. Traore, *The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review*. in: *Information Security and Assurance*, Springer Berlin Heidelberg, 2011, p. 87-100.

investigative, senza però entrare nel merito dell'indagine stessa.

Il rinvenimento di un frammento di DNA sulla scena del crimine, ad esempio, colloca in quella stessa scena, senza ombra di dubbio, la persona a cui quel profilo genetico appartiene, senza però fornire un quadro temporale od una interpretazione di quella presenza nel contesto investigato.

La stessa persona potrebbe avere una giustificazione logica e plausibile (alibi) che motivi la sua presenza sulla scena, senza per forza essere collegata all'evento criminoso.

E' compito degli investigatori definire il contesto spazio-temporale assumendo prove, escutendo testimoni, piuttosto che rilevando elementi che possano avvalorare l'alibi fornito.

Il biologo forense fornisce esclusivamente un elemento di valutazione a seguito di esami scientifici, senza però interagire direttamente nell'attività di polizia giudiziaria.

Lo scienziato, lo specialista, l'esperto, il tecnico, forniranno spiegazioni sulla base di conoscenze scentifiche, elementi che dovranno essere collocati in un contesto investigativo, al fine di fornire un ausilio od un riscontro alle ipotesi formulate nel corso delle indagini.

Risulta differente, come si argomenterà nel prosieguo, nelle attività d'indagine compiute a livello informatico o che comunque contemplino l'analisi delle evidenze informatiche come fondamento per un'ipotesi accusatoria: l'obiettivo dell'investigatore forense in ambito digitale è proprio quello di individuare, acquisire, analizzare e correlare il dato informatico con tutti gli elementi, materiali ed immateriali, raccolti nel corso delle indagini, pur non perdendo di vista i dettami finalistici di genuinità ed integrità dell'evidenza stessa.

Fulcro di tutta l'attività è il concetto di correlazione che, semanticamente, richiama il più ampio concetto di inferenza, ovvero un ragionamento logico deduttivo da cui si trae una conseguenza da una o più premesse.

A maggior chiarezza della tesi proposta, risulta quanto meno opportuno soffermarsi sulla differenza che intercorre tra dato ed informazione vera e propria.

Si è già accennato come alcuni autori abbiano fornito più di una interpretazione delle attività tipiche di *computer forensics*, definendole tra l'altro come un complesso di tecniche tese alla "*manipolazione controllata dei dati e delle informazioni"*[16].

Nel linguaggio comune, l'informazione può essere definita come un elemento che permette di addivenire alla conoscenza di qualcosa; mentre il dato potrebbe essere definito come un elemento conosciuto o conoscibile.

In informatica, invece, un dato è un elemento informativo, costituito da simboli che devono essere elaborati: l'elaborazione dei dati produce informazioni.

Ad esempio, il dato "*Bianchi*" esprime un cognome, il dato "*Mario*" un nome, il dato "*BNCMRR83B01L219X*" un ipotetico codice fiscale. Se l'utente interroga un database per sapere quale sia il codice fiscale dell'utente *Mario Bianchi*, i tre dati costituiscono una informazione.

Questo preambolo definitorio diviene utile per comprendere come nelle indagini informatiche non sia necessaria la mera estrazione dei dati

[16] G. Costabile, *Computer forensics e informatica investigativa alla luce della Legge n.48 del 2008*, *cit.* p. 465.

presenti all'interno di un qualsiasi dispositivo di memorizzazione, bensì risulti fondamentale che un'attenta disamina di tali dati generi un'informazione, ovvero produca, in termini giuridici, un elemento indiziario o, ancor meglio, una fonte di prova. Tale analisi deve necessariamente essere effettuata all'interno del contesto investigativo, correlando e comparando la molteplicità di evidenze presenti nel complesso dell'indagine stessa.

Non si può poi non tenere in considerazione quanto, sempre di più, mondo reale e realtà virtuale interagiscano tra loro, ed il già labile confine tra i due elementi diventerà sempre più lasco ed inconsistente nel prossimo futuro. La quotidianità è scandita dall'alternarsi tra realtà fisica e mondo digitale: interagiamo costantemente attraverso *social network*, *e-mail*, sms, *instant messages*, usando pc, *smartphone*, lettori mp3, *tablet*, etc.[17].

Competenze informatiche ed elevate capacità investigative devono dunque essere alla base delle conoscenze dell'investigatore informatico proprio perché, in questo ambito, non può essere sufficiente una fredda e spersonalizzata analisi di prove scientifiche in quanto le evidenze devono obbligatoriamente essere collegate ai fatti reato ed agli eventi accaduti. Spingendosi oltre, immaginando scenari futuri, si potrebbe auspicare come la figura dell'investigatore comune debba obbligatoriamente possedere competenze tecniche tali da poter comprendere ed analizzare scenari informatici sempre più complessi, poiché sempre più complessa sarà la realtà tecnologica quotidiana.

La balistica, la comparazione delle tracce lasciate sulle superficie dai dermatoglifi, l'estrazione ed il confronto del DNA da liquidi corporei, rilevati sulla scena del crimine, sono strumenti fondamentali per l'analisi del luogo del delitto, per determinare le dinamiche dell'evento, finanche per individuarne il responsabile.

La criminalistica, intesa come metodo scientifico applicato alle indagini criminali, fornisce un contributo importantissimo ed oramai irrinunciabile all'attività dell'investigatore, è però a quest'ultima figura che si richiede una spiccata capacità di astrazione e l'intuito necessario per portare a termine l'attività d'indagine.

Il biologo forense può rilevare le tracce di DNA di un soggetto sulla scena del crimine, fornendo dunque il contesto spaziale, ma è l'analisi spazio-temporale ed il collegamento con altri elementi indiziari che determinano se quello stesso soggetto può essere o meno coinvolto nel fatto criminoso. Tali analisi spettano all'investigatore e non allo scienziato, anche se questi può appartenere ai ranghi di reparti specialistici delle forze di polizia.

Le attività di polizia scientifica hanno senso solo se contestualizzate in una più articolata analisi di tutte le evidenze raccolte a livello investigativo. In ambito digitale le evidenze potrebbero essere reali

[17] Si pensi come sempre di più il vincolo con le nuove tecnologie interviene a modificare la nostra quotidianità, a quanto invasivi possano essere determinati dispositivi o talune applicazioni: scattando una foto con uno *smartphone* ed inviandola sul proprio profilo di un qualsiasi *social network* possiamo trasmettere la nostra immagine, le nostre coordinate geografiche, gli "stati d'animo" del momento…informazioni sulla nostra vita reale convogliate attraverso una realtà virtuale che sempre di più acquisisce fisicità e concretezza. Persone, luoghi, circostanze, situazioni reali possono costituire il classico alibi, analogamente messaggi istantanei, *log*, coordinate gps, transazioni elettroniche, accessi a caselle di posta elettronica o profili *social network* possono costituire il cd. alibi informatico.

o virtuali, discrete o fisiche, ma tutte correlabili tra di loro[18].

D'altro canto potrebbe essere oltremodo superfluo sottolineare come non sia necessario che l'investigatore possegga le competenze scientifiche per poter analizzare le basi azotate dell'eventuale frammento di DNA rilevato sulla scena, ma è senza dubbio importante che lo stesso investigatore debba comprendere come determinate informazioni possano essere reperite in un contesto digitale o in una realtà virtuale.

Una qualsiasi attività d'indagine che vede coinvolti elementi ad alto impatto tecnologico richiede una sinergica collaborazione tra analista ed investigatore. Per tale motivo è pressoché auspicabile che queste due figure siano vincolate da uno stretto mandato collaborativo o, ancor meglio, vengano identificate in una sola persona.

Solo un attento investigatore può avere la possibilità di verificare, sempre e comunque, ogni indizio rilevato; per converso, solo un esperto analista forense di sistemi informativi dispone delle necessarie competenze per evidenziare le minime tracce lasciate su un elaboratore.

3. Legge 18 marzo 2008 nr. 48 e Best Practices per l'acquisizione della prova informatica.

L'intrinseca fragilità che caratterizza le prove digitali le rende facilmente soggette ad alterazioni o modificazioni anche da parte degli stessi investigatori che, se non adeguatamente preparati, possono compromettere e inquinare, anche inconsapevolmente, la *scena criminis*.

La fase più delicata è sicuramente quella riferibile alla repertazione e all'acquisizione degli elementi di prova di natura digitale: qui le difficoltà interpretative della realtà informatica si ripercuotono inevitabilmente sull'applicazione dei diversi istituti giuridici che normalmente vengono utilizzati per acquisire e conservare le prove di un crimine.

Raramente in passato la gestione della prova informatica rispecchiava i requisiti minimi imposti dalla comunità scientifica internazionale e certamente l'assenza di una specifica disciplina codificata non facilitava il giudizio della sua ammissibilità o utilizzabilità in sede dibattimentale.

L'entrata in vigore della legge 18 marzo 2008 n. 48 ha di fatto sancito l'introduzione dei principi fondanti della *computer forensics* all'interno del nostro ordinamento, prevedendo importanti aspetti legati alla gestione di quegli elementi di prova che, per loro natura, presentano caratteristiche di estrema volatilità e fragilità[19].

[18] Ci si riferisce a solo titolo di esempio alla correlazione di elementi differenti quali *file di log*, tabulati telefonici o telematici, transazioni elettroniche, etc. tutti attribuibili al medesimo soggetto fisico.

[19] Con legge 18 marzo 2008 n. 48, pubblicata in Gazzetta Ufficiale il 4 aprile 2008 n. 80, S.O. n. 79, è stata recepita la Convenzione di Budapest sulla criminalità informatica. La Convenzione si compone di tre distinte sezioni: una prima finalizzata all'armonizzazione di norme di diritto sostanziale tra i vari Stati firmatari al fine di garantire l'omogeneità delle incriminazioni; una seconda parte dedicata alla disciplina processuale ed all'innovazione degli strumenti investigativi da applicare all'acquisizione probatoria delle evidenze digitali; ed una terza, che pone le basi per una concreta e fattiva collaborazione tra gli Stati, snellendo le procedure *rogatoriali* di assistenza giudiziaria internazionale, al fine di una riduzione delle tempistiche di accesso agli elementi di prova in materia di *cyber crimes.* Per un'approfondita disamina sulle innovazioni introdotte nel codice di rito in termini di Computer forensics ad opera del recepimento nel nostro ordinamento della Convenzione di Budapest su Computer Crimes con L.48/2008, si veda *inter alia:* F. Bravo, "Indagini informatiche e acquisizione della prova nel processo penale", in *Rivista di Criminologia, Vittimologia e Sicurezza*, vol. III-n.3, vol. IV-n.1, 2009-2010 (numero doppio), pp.

In primo luogo, modificando l'art. 491 bis del codice penale, ha "smaterializzato" il concetto di documento informatico, sottraendolo dal fardello del "supporto"[20] a cui faceva riferimento la formulazione originaria introdotta dalla L. 547/93, rinviando dunque alla medesima definizione introdotta dal Codice dell'Amministrazione Digitale (decreto legislativo 7 marzo 2005, n. 82)[21].

Il provvedimento di ratifica ha poi esplicitamente previsto alcune regole di corretta gestione dell'evidenza informatica. Tali metodologie, seppur da tempo entrate a far parte di una corretta prassi investigativa da parte di reparti specializzati delle forze di polizia[22], non sempre vedevano una loro puntuale attuazione, a scapito di un'altalenante utilizzabilità della prova stessa nelle fasi dibattimentali[23].

Le previsioni introdotte dalla legge 48/2008 possono essere lette come un primo, anche se flebile, approccio a quelle *best practices* tanto care agli ordinamenti di *Common Law*, ma ancor meglio come il recepimento, nell'ordinamento nazionale, dei principi fondamentali di *digital forensics*[24].

Seppur il legislatore si sia mosso cautamente nell'introdurre i nuovi principi per l'assunzione delle prove informatiche, non indicando cioè nel dettaglio le modalità esecutorie da applicare nell'utilizzo di tali istituti in ultimo novellati, si è comunque focalizzata l'attenzione su due basilari aspetti, sicuramente più vincolati al risultato finale che non al metodo da utilizzare, ovvero la corretta procedura di copia dei dati utili alle indagini e la loro integrità e non alterabilità in sede di acquisizione.

Un primo riferimento alle migliori pratiche, finalizzate alla corretta conservazione dei dati, è riscontrabile già all'articolo 8 della citata legge che, modificando le previsioni dell'art. 244 del codice di rito, introduce la locuzione "*anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*".

Come è noto l'art. 244 c.p.p., inserito nel Libro III, Titolo III del codice, individua i casi e le forme delle ispezioni come mezzi di ricerca della prova.

Tale istituto, precedentemente al recepimento della Convenzione di Budapest sui *Computer*

231-245, e ancora G. Ziccardi, "L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche", in L. Luparia (a cura di), *Sistema penale e criminalità informatica*, Giufrè, Milano, 2009, pp. 165-180.

[20] Il secondo comma dell'art. 491 *bis*, abrogato dalla L. 48/2008, recitava: "*A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli*".

[21] L'art. 1 let. *p* del d.lgs. 82/2005 definisce "*documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*".

[22] Tali prassi investigative venivano esclusivamente utilizzate, anche se in maniera autonoma e non standardizzata, dai vari reparti specializzati delle forze di polizia attivi in indagini ad alto impatto tecnologico, quali Polizia Postale e delle Comunicazioni, RACIS, GAT, etc.

[23] Si pensi ad esempio alle sentenze del Tribunale di Chieti del 2 marzo 2006 e n. 1369/2006 del Tribunale di Pescara, dove in entrambi i casi una non corretta e formale acquisizione di elementi di prova digitale hanno contribuito all'assoluzione degli indagati.

[24] Per *Best Practices* si intende quell'insieme di comportamenti, non necessariamente formalizzati e codificati, che vengono considerati dalla comunità scientifica come il miglior modo o il modo più corretto di operare, per svolgere attività ambito scientifico e/o tecnologico. Nel caso specifico ci si riferisce a tutto quel complesso di procedure e modalità di esecuzione, avvalorate dalla comunità scientifica, da enti di ricerca, agenzie governative o associazioni di categoria, al fine di individuare, rilevare, acquisire, gestire, documentare

Crimes, non menzionava la possibilità di estendere la ricerca delle tracce o degli effetti materiali del reato ai sistemi informatici e telematici[25].

I cardini di tale modifica, inseriti in egual misura anche nelle previsioni dei successivi articoli del codice di procedura penale che individuano gli altri mezzi di ricerca della prova, sono sicuramente da individuarsi nella necessità di adottare adeguate misure tecniche che consentano una corretta conservazione dei dati acquisiti, nonché di ricorrere a procedure tali da garantirne la genuinità e la non alterabilità nella fase esecutoria dell'atto stesso[26].

I due aspetti, anche se strettamente correlati tra loro, individuano concetti ben distinti che possono essere apprezzati in relazione alle finalità che ci si aspetta di soddisfare.

A tal riguardo è stato rilevato che "*In primo luogo vi è la sacralità della conservazione dei dati originali, sia in previsione di ulteriori analisi eventualmente necessarie in futuro sia, più semplicemente, nell'ottica di garantire che, anche a distanza di mesi od anni, ci possa essere sempre la possibilità, per le parti processuali, di riferirsi e di confrontarsi con i dati originali*"[27].

Il secondo importante punto fa riferimento all'inalterabilità del dato nel suo complesso: il legislatore, nell'introdurre questo fondamentale vincolo, individua correttamente l'estrema labilità della traccia digitale, imponendo dunque idonee misure che vadano ad evitare ogni minima sua alterazione, anche qualora si operi in regime di estrema urgenza[28].

Anche quanto le condizioni di tempo e di luogo impongono un'attività di iniziativa da parte della Polizia Giudiziaria per evitare o limitare la dispersione o l'alterazione di cose o tracce inerenti al reato, vi è comunque la previsione di utilizzare le corrette procedure di *computer forensics* al fine di acquisire correttamente l'evidenza digitale.

Altra importante modifica introdotta dalla legge di ratifica della Convenzione riguarda l'art. 247 c.p.p., laddove un'attività orientata alla ricerca del corpo del reato o "cose" pertinenti al reato vede

---

e presentare in maniera certa e non distruttiva una evidenza digitale.

[25] Il testo dell'art. 244 C.P.P. prima dell'entrata in vigore della L. 48/2998, recitava: "*L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato. 2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica.*"

[26] I mezzi di ricerca della prova, regolati nel Libro III, Titolo III del vigente codice di procedura penale, costituiscono tutte quelle attività che sono finalizzate all'acquisizione diretta o indiretta della prova, per mezzo dell'individuazione dei mezzi di prova o, indirettamente, delle fonti di prova per il dibattimento. Più precisamente sono attività svolte in fase predibattimentale consistenti nella ricerca di persone o cose e nell'individuazione di luoghi che possano risultare utili per la dimostrazione del fatto costituente reato e necessari per l'acquisizione delle fonti di prova.

[27] G. Ziccardi, "L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche", in L. Luparia (a cura di), *Sistema penale e criminalità informatica*, Giufrè, Milano, 2009, p. 167.

[28] La novella dell'art. 354 C.P.P. evidenzia l'importanza di una corretta acquisizione della prova digitale anche quando sussistano ragioni di urgenza, infatti al secondo comma del citato articolo si legge: "*In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità*".

un ampliamento dello spettro esecutorio anche ai sistemi informatici o telematici, ancorché *protetti da misure di sicurezza*, mantenendo, anche in questo caso invariata, la disposizione quasi dogmatica dell'adozione di *misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*[29].

Analoghe modifiche compaiono altresì nella previsione della perquisizione d'iniziativa della P.G. di cui all'art.352 c.p.p., evidenziando ancora, come per il già citato dispositivo di cui all'art. 354 c.p.p., che le esigenze d'urgenza non possano prevalere sull'obbligatorietà dell'utilizzo di metodologie quantomeno di carattere *forensically sound*[30].

L'adozione dunque di procedure atte a salvaguardare il dato nella sua interezza, salvo ipotesi estreme legate a cause di forza maggiore, dovranno quindi entrare obbligatoriamente nella prassi quotidiana per tutti quegli operatori specializzati e non che si troveranno di fronte l'onere dell'acquisizione di evidenze digitali[31].

Rimane da chiedersi quali potrebbero essere, a questo punto, le conseguenze processuali previste in ordine alla non adozione delle misure tecniche idonee alla salvaguardia del dato.

"Le modifiche introdotte dalla legge di ratifica appaiono ad una prima disamina esenti da previsioni sanzionatorie e dunque lacunose nella determinazione di quali effetti conseguono al mancato rispetto di tali prescrizioni"[32].

La mancanza di un'ipotesi sanzionatoria specifica, in ordine alla non adozione di buone pratiche, non può essere di certo considerata un problema marginale in quanto, a differenza delle modalità a cui si perviene alla prova scientifica, non codificata, ma sottoposta a giudizio di

[29] Il testo dell'art. 247 C.P.P. innovato dalla L.48/2008 recita: "*1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta la perquisizione locale. 1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione."*

[30] Buona parte della letteratura americana individua il concetto di *foreniscally sound*, per indicare tutte quelle procedure di *computer forensics* che, per varie motivazioni, legate sia all'urgenza di compiere determinati atti, ovvero alla tipologia di evidenze da repertare, tendono alla corretta applicazione delle *best praticies*, pur non potendo garantire l'assoluta ripetibilità ed integrità. E' questo il caso ad esempio della *mobile forensics* o delle attività di ricerca della prova su dispositivi *embedded*.

[31] Come accennato in precedenza, ancor prima dell'introduzione dei dettami normativi apportati dal recepimento della Convenzione di Budapest, alcuni reparti specializzati delle forze di polizia disponevano già del *know how* necessario e di procedure tese a garantire l'inalterabilità e la genuinità dell'evidenza digitale. Tali procedure però non sono paragonabili a vere e proprie *best practices* "nazionali" poiché non presentano i caratteri di pubblicità, di generale condivisione e di recepimento o accettazione da parte della comunità scientifica. Come si accennerà in seguito, il Servizio Polizia Postale e delle Comunicazioni, negli anni, ha prodotto circolari ad uso interno indirizzate ai propri operatori, al fine di fornire indicazioni su come approcciarsi a specifiche attività investigative in ordine all'acquisizione di determinate evidenze informatiche. Lo stesso Servizio, come del resto l'Arma dei Carabinieri ed anche il Comando Generale della Guardia di Finanza, hanno da tempo promosso e sviluppato un percorso di aggiornamento professionale e di interscambio esperienziale con omologhe agenzie straniere, indirizzato agli operatori impiegati in servizi ad alta specializzazione tecnica e volto ad acquisire le competenze specialistiche necessarie con diretto riferimento anche alle *best practices* internazionali.

[32] D. La Muscatella, "La ricerca della prova digitale e la violazione delle best practices : un'attività investigativa complessa tra recenti riforme e principi consolidati", in *Ciberspazio e Diritto*, n. 2, 2011, p. 222.

ammissibilità[33], per la prova digitale, vi è comunque la previsione dell'utilizzo di particolari metodologie a sua garanzia, senza una esplicita indicazione in termini di utilizzabilità di tale evidenza in sede processuale qualora non vengano seguite specifiche prassi.

La mancanza di una precisa sanzione assume particolare rilevanza nella prospettiva del difensore che, di fronte ad un'acquisizione della *digital evidence* compiuta con modalità approssimative, si potrebbe trovare nelle condizioni di eccepire la violazione delle disposizioni di legge, insistendo per un giudizio di non ammissibilità a causa dell'attività irrituale degli inquirenti.

4. *Computer Forensics*: fasi e principali metodologie d'intervento.

L'eterogeneità di supporti elettronici che possono celare tracce e indizi, la costante innovazione tecnologica e finanche le molteplici situazioni in cui un investigatore deve confrontarsi, non permettono di individuare una procedura univoca ed universale per l'acquisizione della prova digitale.

Si pensi ad esempio ai primi e necessari accertamenti sulla scena del crimine dove, oltre alle comuni tracce da repertare, si evidenziano supporti informatici, dispositivi elettronici di varia natura, computer e quant'altro; oppure nell'ambito dell'esecuzione di un decreto di perquisizione locale negli uffici di una qualsiasi azienda dove non è insolito trovare sistemi informatici estremamente complessi sia per costruzione sia per applicativi o sistemi operativi installati[34].

Gli scenari possibili potrebbero essere innumerevoli e comunque pur sempre differenti gli uni dagli altri.

Molteplici altresì potrebbero essere le tipologie di evidenze elettroniche da individuare e repertare.

In alcuni casi proprio l'individuazione, ancor prima di una corretta acquisizione, pone numerosi e complessi problemi all'investigatore non esperto e non aduso alle nuove tecnologie. In un contesto investigativo non esclusivamente digitale si potrebbe immaginare come, prima ancora dell'acquisizione, possa essere difficoltosa l'individuazione di elementi probatori nel contesto del fatto investigato che, ad una puntuale e più attenta analisi successiva, potrebbero rivelare evidenze importantissime.

I numerosi fatti di cronaca dimostrano come una corretta analisi delle evidenze informatiche possa corroborare un'ipotesi investigativa a scapito di un presunto alibi fornito dall'imputato.

Il riferimento ai noti fatti di Perugia[35] , dove una corretta e circostanziata analisi delle attività di un computer portatile, in uso ad uno degli imputati, ha permesso di evidenziare incongruenze nelle dichiarazioni fornite dagli stessi in sede di interrogatorio prima e, successivamente, confermate in dibattimento, è illuminante dal punto di vista dell'applicazione, quasi pedissequa, di una metodologia operativa ineccepibile, per lo meno dal punto di vista delle indagini digitali.

[33] Si rammenta quanta importanza abbiano avuto le sentenze, in particolare nei sistemi di *common law*, della c.d. *cultura dei criteri* (nel 1993, *Daubert v. Merrel Dow Pharmaceutical, Inc., 113S. Ct.2786*, seguita poi, nel 1999, dalla sentenza Kumho Tire v. Carmichael, *526 U.S. 137*) che subito trovò spazio anche nel nostro sistema (cfr. Cass. Pen., V, 09.07.1993).

[34] Per comuni tracce da repertare si devono intendere tutti quegli elementi di natura organica e non, tipici e presenti in una scena del crimine.

[35] Per una disamina dei fatti di cronaca legati all'omicidio di Meredith Kercher si rimanda tra gli altri

Analogamente, una non corretta repertazione e una ben più farraginosa analisi di analoghi supporti ha evidenziato come in un contraddittorio tra le parti possa rivelarsi fondamentale al fine di demolire un complesso castello accusatorio basato però su prove meramente indiziarie[36].

Per assumere valore probatorio l'evidenza digitale dovrà soddisfare alcuni requisiti fondamentali, che svolgono il ruolo di condizioni imprescindibili per una corretta utilizzabilità della prova stessa.

Una accurata applicazione delle procedure di *digital forensics* tenderà ad assicurare quei requisiti di integrità, autenticità, veridicità, non ripudiabilità e completezza della prova.

Tali procedure dovranno garantire che quanto individuato, acquisito e successivamente analizzato, corrisponda esattamente a quanto riscontrato nel momento dell'intervento sulla scena.

Ancor prima di dare risalto alle migliori pratiche da utilizzare per poter gestire la prova informatica nella maniera più corretta, corre l'obbligo di fornire alcune indicazioni in merito alle fasi che tipizzano in via generale un'attività di *digital forensics*.

Tali momenti rispecchiano per lo più le procedure classiche e già consolidate dell'investigazione criminale o, meglio ancora, quelle metodologie di approccio al teatro operativo che un qualsiasi investigatore dovrebbe seguire al fine di repertare elementi utili alle indagini stesse.

I passaggi che caratterizzano l'attività di *computer forensics* possono essere riassunti nell'individuazione, preservazione, acquisizione, analisi e correlazione dei dati assunti, oltre che in una completa ed esaustiva documentazione di quanto effettuato nelle singole fasi.

A corollario di tali passaggi è bene evidenziare il ruolo di primaria importanza che riveste la gestione dell'evidenza informatica nelle singole fasi investigative e processuali.

L'immaterialità dell'evidenza digitale si scontra indubbiamente con la materialità tipica del supporto ove questa risulta memorizzata. Sebbene per alcune tipologie di supporti la loro individuazione non dovrebbe risultare difficoltosa, per esempio nel caso in cui ci si trovi di fronte a *floppy-disk*, *pen-drive*, *hard-disk*, ovvero memorie allo stato solido quali *SD, Compact Flash*, etc.; vi è però da soffermasi sulle problematiche relative all'individuazione di dispositivi non semplicisticamente identificabili come tali.

A tal riguardo le maggiori difficoltà non intervengono nel momento in cui l'investigatore si trovi davanti a dispositivi di tipo "comune", ovvero evidenze rilevate all'interno di dispositivi elettronici di comune utilizzo, ma già quando s'incontrano supporti che contengono evidenze di

a: V.M. Mastronardi, G. Castellini, *Meredith: luci e ombre a Perugia*, Armando, Roma 2009;

[36] Un esempio in negativo di come una non corretta applicazione delle più basilari norme di *computer forensics* possa divenire la chiave di volta per screditare una complessa attività investigativa, potrebbe essere l'ormai triste e noto caso legato all'omicidio di Chiara Poggi. La motivazione della sentenza di primo grado, che ha assolto Alberto Stasi, unico imputato in quell'omicidio, affronta il tema della gestione delle prove digitali in maniera molto diretta, infatti in uno dei passaggi più importanti della disamina delle prove informatiche, si può leggere: "*E qui affrontiamo uno dei capitoli più critici dell'intero procedimento. In data 14 agosto 2007 Stasi Alberto consegnava spontaneamente alla polizia giudiziaria il proprio computer portatile (marca "Compaq"). Da quel momento fino al 29 agosto 2007, quando il reperto informatico veniva consegnato ai consulenti tecnici del pubblico ministero che procedevano all'effettuazione delle copie forensi dello stesso, i carabinieri accedevano ripetutamente e scorrettamente (senza l'utilizzo, cioè delle necessarie tecniche forensi di indagine) alla quasi totalità del contenuto del*

tipo "nascoste", che contengono elementi memorizzati all'interno di supporti non tradizionali, o "celate", presenti in supporti creati *ad hoc*[37]. Le difficoltà di una corretta individuazione dell'evidenza digitale aumentano in maniera esponenziale, con proporzione inversa però, rispetto alle competenze tecniche e all'esperienza degli operatori che compiono il sopralluogo.

La fase cronologicamente successiva all'identificazione del reperto consiste nella preservazione e isolamento dello stesso dal mondo esterno.

Tale accorgimento risulta ancor più necessario quando l'evidenza informatica, la prova o, meglio ancora, il dato oggetto della ricerca risulti essere memorizzato all'interno di supporti volatili o ad accesso randomico (tipicamente i dati memorizzati nella RAM, o nella *cache* di sistema).

E' questa l'ipotesi in cui l'evidenza sia, per esempio, individuabile nell'attualizzazione di un dato di traffico che contempli le connessioni attive in quel momento sul sistema informatico oggetto di perquisizione (*router*, *server*, etc.).

Nella pratica si potrebbe immaginare il caso in cui vi sia la necessità di eseguire una perquisizione per fattispecie relative alla diffusione di materiale pedopornografico, ovvero alla detenzione di ingente quantità[38] dello stesso materiale (art. 600 *ter* e *quater* c.p.), dove la dimostrazione della flagranza prevede l'applicazione della misura precautelare dell'arresto facoltativo, così come previsto dall'art. 381 c.p.p.

Un non corretto isolamento del sistema comporterebbe una non precisa acquisizione della fonte di prova e, dunque, la non dimostrabilità della condotta illecita e la impossibile applicazione della misura stessa.

Risulta alquanto ovvio indicare come la corretta preservazione del reperto non sia di esclusiva pertinenza dei soli dati volatili o temporanei, essa deve infatti essere applicata a tutti i reperti digitali rinvenuti sulla scena.

Le procedure di repertazione ed isolamento contemplano una fase descrittiva, che prevede il sopralluogo con un puntuale inventario delle evidenze rinvenute, ed una fase tecnica, che ha lo scopo di impedire qualsiasi interazione dei reperti con l'ambiente circostante sino alla successiva fase di acquisizione.

Il personale impegnato nel sopralluogo o nella ricerca dovrà aver cura di documentare, per ogni

computer".

[37] Per un approfondimento maggiore inerente la suddivisione delle tipologie di tracce digitali rinvenibili all'interno della scena del crimine si rimanda *a* '*Digital evidence field guide: what every peace officer must know'*, *U.S. Department of Justice, Federal Bureau of Investigation– Regional Computer Forensics Laboratory Program (RCFL) and Computer Analysis Response Team (CART)*, in internet all'indirizzo http://www.rcfl.gov/downloads/documents/FieldGuide_sc.pdf (sito consultato e documento verificato in ultimo in data 14/12/2013).

[38] L'art. 600 *quater*, così come innovato dalla Legge 6 febbraio 2006, n. 38, vede la previsione dell'aumento della pena sino a due terzi, qualora la detenzione di materiale prodotto mediante lo sfruttamento sessuale di minori degli anni diciotto sia di ingente quantità. Per tale motivo, considerando la pena edittale maggiorata, nella flagranza di reato gli ufficiali di P.G. hanno facoltà di applicare la misura precautelare dell'arresto facoltativo, così come disciplinato dall'art.381 C.P.P.. Spesse volte infatti, durante l'esecuzione di deleghe di perquisizioni locali nell'ambito di procedimenti penali in ordine ai reati di cui ai predetti articoli, si ha la facoltà di estendere la perquisizione ai sistemi informatici o telematici rinvenuti nelle circostanze. Tipicamente gli operatori specializzati, eseguano quella che in maniera non del tutto corretta viene definita "*preview*" ovvero, attuando le prescrizioni previste dalla L.48/2008, viene effettuata una perquisizione "informatica" alla ricerca di quegli elementi grafici ritenuti illegali, anche al fine di una successiva valutazione dell'applicazione della custodia *de quo*.

singolo dispositivo, le caratteristiche, lo stato in cui si trova, verificare eventuali collegamenti ed annotare, applicando anche etichette sui singoli cavi[39], la loro disposizione e se possibile, la funzione o lo scopo di quel determinato dispositivo (ad esempio, nel caso di *server* sarebbe opportuno, prima ancora di procedere alla repertazione o alla acquisizione, accertare quali servizi propone: posta elettronica, *web server*, *file server*, etc.).

Dovrà verificare la presenza di "collegamenti" *wireless*, oltre che di cablaggi strutturati, ed assicurare che i sistemi permangano nello stato in cui si trovano fino alla successiva fase di acquisizione[40].

Analogamente tutti i dispositivi spenti al momento del sopralluogo dovrebbero essere riposti in buste antistatiche, per il loro successivo trasporto e analisi in laboratorio.

Una regola fondamentale, forse da considerarsi la norma base di tutte le complesse procedure legate alle attività di *digital forensics*, è quella di evitare nella maniera più assoluta di accedere al dispositivo, ovvero interagire in una qualsiasi maniera con le evidenze rilevate sulla scena[41].

La mera accensione di un computer, di un cellulare o di un qualunque dispositivo che abbia capacità computazionali provoca un'interazione tra dati, memorie e sistema operativo che, in termini di gestione forense dell'evidenza, deve sempre essere considerata come un'alterazione di tali dati e dunque del reperto stesso.

L'acquisizione della prova informatica è sicuramente la fase che presenta una maggior criticità, proprio perché deve garantire l'inalterabilità dell'elemento che viene ad essere repertato e la sua fissazione nel tempo.

Tale procedura non potrà essere attuata come una mera copia del dato ricercato, poiché un'operazione di questo tipo comporterebbe l'irreparabile perdita di tutti quegli elementi che sono a corollario della stessa prova.

Ci si riferisce ad esempio alle indicazioni temporali di creazione del *file*, di sua modifica o di cancellazione; oppure anche a tutti quegli elementi che costituiscono informazioni fondamentali prescindendo dalla parte contenutistica del documento informatico stesso.

L'obiettivo ultimo di una corretta acquisizione della prova informatica è quello di fornire le massime garanzie in termini di integrità, autenticità, veridicità e non ripudiabilità.

Il dato dovrà essere acquisito nella sua integrità e non in maniera parziale o frettolosa, dovranno essere indicati tutti gli elementi collegati alla sua provenienza e dovrà essere cristallizzato (*to freeze*, congelato) al fine di un suo non disconoscimento nelle successive fasi investigativo-dibattimentali.

---

[39] L'applicazione di etichette numerate sui singoli dispositivi e su tutti i cavi di collegamento rinvenuti sulla scena, oltre ad essere una delle primarie e consolidate procedure, ha lo scopo di inventariare ed annotare in maniera puntuale e corretta tutto ciò che si è rilevato. Alla stregua del sopraluogo di polizia scientifica, è molto importante documentare accuratamente la scena digitale anche per una sua successiva ricostruzione in laboratorio.

[40] Come verrà indicato nel successivo paragrafo l'acquisizione deve essere considerata alla stregua della repertazione dell'evidenza. Non sempre le circostanze di tempo e di luogo permettono l'acquisizione in loco e quindi risulta più conveniente repertare il dispositivo per poi acquisirne i dati in laboratorio.

[41] Tale regola è necessaria per evitare una qualsiasi modifica all'evidenza raccolta. Esistono comunque tecniche, definite di *live forensics* utilizzate esclusivamente da personale altamente specializzato, che permettono di acquisire nell'immediatezza elementi utili anche su dispositivi accesi, senza per altro alterarne il loro corretto funzionamento, vedasi *infra*.

Generalmente l'acquisizione dell'evidenza digitale consiste nella creazione della cosiddetta "*bit stream image"*, ovvero nella copia "*bit to bit"* del dispositivo oggetto d'indagine.

Per copia *bit stream*, o immagine forense, si deve intendere una vera e propria clonazione a "basso livello", del dispositivo oggetto di analisi.

In tale fase, la procedura di acquisizione non tiene conto della parte contenutistica del dato, ma della sua struttura fisica e della sua allocazione logica[42].

Per intendere meglio il concetto di copia *bit stream*, si potrebbe astrattamente immaginare di poter leggere in maniera sequenziale tutti i *bit* memorizzati all'interno di un supporto e duplicarli, mantenendo inalterata la loro sequenza e collocazione fisica e logica all'interno di un nuovo dispositivo di memorizzazione, senza preoccuparsi di interpretarne il significato[43].

Una copia effettuata con tali modalità presenterà pertanto la stessa sequenza di dati del supporto originale, comprese le aree che contengono informazioni non più visibili all'utilizzatore di quel sistema[44]. Un'immagine *bit stream* altro non è che il clone esatto del dispositivo o del supporto repertato.

L'analisi della copia *bit stream* permetterà di rilevare, oltre ai dati regolarmente memorizzati, anche porzioni di *file* modificati, *file* temporanei, *file* cancellati e non completamente sovrascritti.

L'introduzione delle norme basilari di *digital forensics* previste dalla già più volte citata legge 48/2008 ha modificato, normativamente parlando, l'approccio dell'investigatore che si trova ad affrontare il processo di acquisizione della prova informatica.

Infatti, in ottemperanza alle prescrizioni di assicurazione e non modifica dell'evidenza informatica, le procedure di acquisizione dovranno orientarsi alla minor invasività possibile.

Nella pratica si dovranno adottare metodologie tecniche, differenziate in base alla tipologia di dispositivo da acquisire, che tenderanno ad un approccio alla prova in modalità *read-only*, ovvero "leggere" il contenuto del dispositivo senza introdurre alcuna modifica su di esso.

Appare utile, a tal riguardo, ricordare come il dato informatico o digitale consista in una successione di *bit*, ovvero di "0" ed "1", memorizzati all'interno di un supporto che può presentarsi in varie forme, composizioni e tecnologie.

I *bit* memorizzati, ove non si adottassero accorgimenti tecnici adeguati, potrebbero essere soggetti a modifiche, anche involontarie, da parte dell'operatore del sistema.

Pertanto nei procedimenti in cui viene prodotta la *digital evidence* dovrà essere presuntivamente considerata la possibilità di una sua eventuale alterazione. Tale presunzione non deve essere intesa come una dichiarazione di generale inattendibilità del dato stesso o delle procedure utilizzate per la sua acquisizione; al contrario, l'utilizzo di tecnologie e strumentazioni adeguate,

[42] L'acquisizione dovrà mirare a duplicare interamente il supporto, mantenendo invariato, per ogni singolo elemento, il percorso di memorizzazione, le dimensioni fisiche e logiche (inteso come numero di settori/cluster occupati e numero di *byte* utilizzati) data ed ora di memorizzazione etc.

[43] Per comprendere meglio il concetto di *bit stream* si potrebbe immaginare un qualsiasi dispositivo di memorizzazione come l'insieme di *bit* , ovvero di stati logici (leggasi «0» e «1»), memorizzati in maniera sequenziale all'interno di un nastro magnetico. Il clone del dispositivo (*bit stream immage*) sarà dunque la copia esatta di tali stati logici su un secondo nastro (*destination*), che presenterà la struttura e la sequenzialità dei singoli bit del primo (*source*).

[44] Sono le cosiddette aree non allocate, lo *slack space*, i

quali ad esempio l'applicazione di funzioni di *hash* e l'utilizzo di sistemi che inibiscono "fisicamente" la modifica del dispositivo (*forensics write blockers*), garantiscono la preservazione del dato stesso e la sua successiva corretta analisi.

La semplice "lettura" di dispositivi di memorizzazione, quali ad esempio i supporti magnetici come *hard disk, floppy disk, memory card, etc.*, potrebbe causare un'alterazione dei dati in relazione, ad esempio, alle informazioni di ultimo accesso, alla data di creazione ovvero di ultima modifica dei *file* ivi contenuti.

Questi elementi, non necessari nel caso di un uso comune dello strumento informatico, potrebbero divenire evidenze fondamentali allorquando le esigenze probatorie rendano necessario l'utilizzo di tali informazioni al fine di dimostrare determinati atti o fatti giuridicamente rilevanti.

L'utilizzo di strumentazione tecnica volta a proteggere eventuali modifiche dell'evidenza nella fase dell'acquisizione è solo uno dei passaggi necessari e fondamentali a garanzia di integrità, autenticità, veridicità e non ripudiabilità.

Acquisita l'evidenza, occorre fornire elementi certi di non ripudio della prova stessa. A questo scopo la cristallizzazione ed il congelamento del dato avverrà attraverso l'utilizzo di dispositivi o di applicativi *software* che, sfruttando funzioni matematiche di algebra modulare conosciute come funzioni di *hash*, genereranno il "sigillo digitale" o l'impronta dell'evidenza stessa.

Nel linguaggio matematico ed informatico, la funzione *hash* è una funzione non iniettiva che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita[45].

La codifica *hash* viene prodotta da un algoritmo che, partendo da un documento arbitrario di qualsiasi tipo e dimensione, lo elabora e genera una stringa univoca di dimensioni fisse denominato *digest* o impronta.

Applicando una funzione di *hash* al contenuto di un *file* o anche ad un intero dispositivo, si ottiene una sequenza alfanumerica di caratteri che rappresenterà l'impronta digitale dei dati memorizzati nel dispositivo.

Si può facilmente intuire come, a meno di collisioni, risulta altamente improbabile che due elementi differenti presentino lo stesso valore di *digest*[46].

Le funzioni di *hash* più frequentemente applicate alla *digital forensics* sono tipicamente individuate nel MD5[47] e nello SHA-1[48].

Applicando l'algoritmo MD5 ad un documento arbitrario, si può calcolare che la probabilità di ottenere collisioni assuma un valore pari a [1,26 × (2^{-64})] , ovvero in base dieci sarà: [2,32428975 × 10^{-19}].

file cancellati ma non sovrascritti, etc.

[45] Per funzione non iniettiva si intende una funzione matematica univoca, unidirezionale e non invertibile.

[46] Due messaggi diversi danno luogo a una collisione quando generano un identico *digest*.

[47] L'acronimo MD5 (*Message Digest algorithm 5*) indica un algoritmo crittografico di *hashing* realizzato da Ronald Rivest nel 1991 e standardizzato con la RFC 1321. Questo tipo di codifica prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra di 128 bit.

[48] In matematica o informatica, con il termine *SHA* si indica una famiglia di cinque diverse funzioni crittografiche di *hash* sviluppate a partire dal 1993 dall'agenzia statunitense *National Security Agency* (NSA) e pubblicate dal *NIST* come standard federale dal governo degli USA. L'acronimo SHA è riferibile a *Secure Hash Algorithm*. Gli algoritmi della famiglia SHA sono denominati SHA-1, SHA-224, SHA-256, SHA-384 e SHA-512, le ultime 4 varianti sono spesso indicate genericamente come SHA-2, per distinguerle dal primo.

Si consideri che studi medici hanno evidenziato che l'ipotetica probabilità di ottenere la medesima sequenza di DNA su soggetti differenti è pari a circa 10^{-18} e, dunque, almeno un ordine di grandezza superiore rispetto all'utilizzo della funzione di *hash*[49]. Il valore probabilistico è ancor maggiore nel caso delle impronte papillari (una probabilità su sedici miliardi di impronte).

Per quanto sopra, l'utilizzo dell'algoritmo MD5, considerato il più "debole" in termini di collisioni dalla statistica inferenziale, soddisfa ampiamente il concetto di cristallizzazione della prova in termini forensi.

Il punto nodale dell'utilizzo di funzioni di *hash* per cristallizzare il dato è che una minima modifica degli elementi acquisiti genererà un *digest* differente rispetto a quello prodotto in sede di acquisizione sul dispositivo originale.

Il valore di *hash* del dato originario sarà dunque il sigillo elettronico dell'evidenza e dovrà essere custodito e documentato in maniera assolutamente precisa.

Una minima alterazione dell'evidenza, producendo una modifica all'impronta digitale o *digest*, sarà sufficiente ad inficiare tutte le fasi successive del procedimento.

L'*hash* di un documento informatico e quello della sua copia *bit stream*, calcolati in sede di repertazione, costituiranno una certificazione inoppugnabile che il contenuto del supporto originale risulti esattamente uguale alla copia acquisita e sulla quale verranno effettuati gli accertamenti tecnici del caso[50].

Prima di fornire alcune indicazioni in merito all'analisi dei dispositivi, occorre soffermarsi su quali siano gli strumenti più adatti all'esecuzione di una corretta copia forense dell'evidenza digitale. Risulta evidente come i possibili scenari operativi possano essere numerosi, tanto quanto sono numerose le diverse tipologie dei dispositivi digitali e dei supporti di memorizzazione[51].

L'acquisizione dell'evidenza digitale è sicuramente da considerarsi come la fase più delicata di tutto il procedimento. Alcuna letteratura in passato attribuiva a tale momento carattere di non ripetibilità, indicando dunque la necessità di operare *ex* Art 360 c.p.p[52].

[49] A. Collins, E. Morton, *Likelihood ratios for DNA identification*, CRC Genetic Epidemiology Research Group, in Proc. Nati. Acad. Sci. Medical Sciences USA, Vol. 91, pp. 6007-6011, June 1994. In rete all'indirizzo http://www.pnas.org/content/91/13/6007.full.pdf (documento verificato da ultimo in data 01/03/2013)

[50] E' opportuno evidenziare che i supporti magnetici possono subire nel tempo minime modificazioni della loro struttura. Questo potrebbe essere dovuto ad una scarsa cura nella repertazione, ad urti o sbalzi termici, ovvero all'esposizione a campi elettromagnetici, ma anche alla vetustà del dispositivo stesso. La variazione anche solo di un *bit*, produrrà una notevole variazione del *digest* di quel dispositivo. Al fine di evitare l'inutilizzabilità della prova nel suo complesso sarebbe opportuno, in sede di acquisizione, effettuare più *digest*, riferibili a singole porzioni ben definite ovvero ai file in esso memorizzati. In questo modo eventuali ed accidentali modifiche del dispositivo repertato, potrebbero al limite inficiare l'utilizzabilità di quella specifica porzione di disco o *file* che presenta un *hash* differente ma non l'intero dispositivo.

[51] Si pensi come potrebbero essere differenti le procedure di acquisizione se si dovessero applicare ad un elaboratore spento con possibilità di accesso diretto ai dischi di sistema, a un server aziendale che deve fornire importanti servizi nelle 24h e dunque non vi è la possibilità di interruzione dell'operatività a meno di causare elevatissimi danni anche di tipo economico. Si pensi altresì di acquisire dati da sistemi informatici dove per ragioni costruttive non si ha diretto accesso (fisico) ai dischi o alle unità di memorizzazione (EEPC con dischi in SSD *et simila*). Si consideri anche di dover accedere a sistemi di *cloud computing*, in cui la risorsa da acquisire può essere dislocata "ovunque" nel *cyberspazio*.

[52] L'art. 360 C.P.P. (accertamenti tecnici non ripetibili) richiamando direttamente la previsione dell'art.359 C.P.P. (consulenti del Pubblico Ministero), prescrive specifiche garanzie qualora fosse necessario effettuare

E' indubbio che l'acquisizione presenti delle criticità notevoli ma, come si è evidenziato, utilizzando adeguata tecnologia e seguendo le procedure indicate dalle migliori pratiche risulta possibile effettuare una copia forense in termini di assoluta ripetibilità.

Un ben più importante dilemma affligge da anni numerosa dottrina anche autorevole che rileva dubbi sull'utilizzabilità in dibattimento di determinate evidenze acquisite in modo non "trasparente". Tali dubbi sono legati alla libera scelta di utilizzare determinati *software* commerciali di cui non è possibile conoscere a priori il loro codice sorgente.

Si è sostenuto, in particolare da Monti, che utilizzare software commerciali, o meglio ancora a "codice chiuso", non permetta l'effettiva valutazione alle parti delle specifiche del sistema utilizzato e, in particolare, del suo corretto funzionamento in termini di una giusta acquisizione dal momento che "*non essendo possibile analizzare i codici-sorgente di questi programmi, la validità dei report da loro generati è fondata su un vero e proprio atto di fede*"[53].

Fuor d'ogni preconcetto sull'uso di prodotti commerciali ai fini dell'acquisizione forense, appare comunque corretta tale doglianza proprio perché, non avendo la possibilità di analizzare gli algoritmi utilizzati dagli sviluppatori per produrre tali *software*, si ha la preclusione di conoscibilità del loro funzionamento e dunque di ottenere le necessarie garanzie ai fini dibattimentali.

L'estrema fragilità e volatilità dell'evidenza informatica necessita di una gestione il più possibile trasparente e chiara, proprio per non dar adito alle parti di eccepire rilievi di non utilizzabilità.

Sebbene la normativa non imponga alcun vincolo sul software da utilizzare, appare comunque evidente che far riferimento a prodotti il cui codice potrebbe in qualsiasi momento essere sottoposto a verifica possa fornire una maggior e migliore garanzia a tale scopo.

Spesso l'utilizzo dei numerosi applicativi presenti sul mercato e specifici per le attività di *digital forensics* è lasciato alla libera scelta dell'operatore di P.G. piuttosto che del perito o del consulente, sia esso d'ufficio o di parte.

Sarebbe auspicabile a tal proposito la previsione di un ente certificatore che possa accertare in maniera scientifica l'affidabilità dei singoli prodotti disponibili, siano essi commerciali, siano essi *open source*.

Gli Stati Uniti, precursori della materia, demandano da tempo al NIST (*National Institute of Standards and Technology*) tale attività di certificazione che, pur non essendo vincolante, sicuramente fornisce una indicazione importante a cui l'organo giudicante può far riferimento nel momento in cui venga chiamato a stabilire l'utilizzabilità degli elementi acquisiti[54].

L'analisi dell'evidenza informatica è la fase, di tutto il processo legato alle indagini digitali, nella quale maggiormente emergono le competenze tecniche e l'intuito investigativo.

accertamenti tecnici in cui stato delle persone, delle cose e dei luoghi sia soggetto a modificazione.

[53] A. Monti, *Attendibilità dei sistemi di computer forensic*, 2003, p. 2, in rete all'indirizzo http://www.ictlex.net/?p=287 (documento consultato in ultimo in data 18/11/2013).

[54] Il NIST è l'acronimo che identifica il *National Institute of Standards and Technology*, un'agenzia statunitense costituita nel 1901 con lo scopo di definire gli standard tecnologici per il governo americano.

Risulta difficile riuscire a fornire una descrizione succinta, seppur esaustiva, di tale passaggio senza per forza dover addentrarsi in tecnicismi fuori luogo per questa dissertazione.

E' bene comunque indicare come l'analisi dovrà valutare primariamente la prova acquisita nel suo complesso, evidenziandone le caratteristiche salienti: sistema operativo, programmi o applicativi presenti, date di installazione, di utilizzo, ultimo accesso e ultimo spegnimento del dispositivo, utenti presenti e relativi privilegi di accesso, etc.

Occorrerà poi verificare la presenza di sistemi ad accesso condizionato o l'uso di *password*, l'eventuale stato di aggiornamento del sistema, nonché il livello di sicurezza presente (antivirus, firewall etc.).

Tipicamente l'analisi di un dispositivo elettronico, quasi in analogia con il sopralluogo di Polizia Scientifica, dovrà procedere dal generale al particolare, al fine di poter fornire in maniera puntuale ogni eventuale elemento utile.

Si inizierà con una descrizione del sistema sino ad arrivare al singolo applicativo o al *file* oggetto di ricerca, ma anche alle aree cancellate, non più utilizzate, non allocate, sino allo *slack space*, etc.[55]

Diversamente dall'acquisizione, dove risulta possibile definire procedure standard per operare in piena sicurezza, non è altrettanto possibile per l'analisi in quanto volta per volta gli elementi da ricercare potrebbero essere differenti.

E' opportuno ribadire come l'analisi debba essere effettuata su una copia dell'evidenza acquisita al fine di garantire la non alterabilità della prova stessa. Analogamente, in certe circostanze, sarebbe preferibile produrre più di una copia forense al fine di aver sempre a disposizione una copia lavoro su cui effettuare l'esame[56].

Questa fase presenta, per sua natura, caratteristiche di assoluta ripetibilità proprio perché si opera su "copie" precedentemente acquisite e non sull'originale; dunque una eventuale distruzione della copia non comporterà la perdita dell'evidenza stessa.

A tale riguardo non sussistono particolari necessità nell'utilizzazione di specifici applicativi al fine di effettuare un'analisi esaustiva anche se, senza dubbio, sono presenti sul mercato prodotti

[55] E' bene ricordare che ogni singolo *file*, ovvero un insieme logico di dati omogenei e strutturati, viene memorizzato su un qualsiasi supporto magnetico in singole unità elementari denominate *cluster*. Il cluster rappresenta l'unità minima di allocazione dello spazio di un disco. La sua dimensione varia dai 512 Byte ai 32 KByte, a seconda della dimensione del disco e del tipo di codifica (*File System*) utilizzato dal Sistema operativo (S.O.) per inizializzare il disco e renderlo utilizzabile. La parte non-allocata di un supporto informatico è quella zona non utilizzata ed apparentemente vuota che può contenere tracce di precedenti dati rimossi. Le sezioni del disco non-allocate sono accomunate dal fatto di non contenere dati leggibili con i normali mezzi a disposizione dell'utente. Queste aree possono presentare parti non registrate (quindi mai scritte dal sistema), parti usate dal sistema per memorizzazioni temporanee (per esempio quando, all'interno di un programma di scrittura, digitiamo del testo senza memorizzarlo) oppure anche parti contenenti dati cancellati. Se i dati cancellati non sono stati sovrascritti (casualmente dal sistema o volontariamente dall'utente per mezzo di programmi appositi), allora è possibile analizzarli ed anche recuperarli. Lo *slack space* rappresenta la somma delle singole frazioni di *cluster* che non contengono informazioni direttamente riconducibili al singolo file.
Se per esempio un *file* ha una dimensione tale da occupare un certo numero di *cluster*, più una frazione, questa "frazione" viene memorizzata necessariamente su un *cluster* intero che quindi conterrà parte di informazione relativa al *file* e parte di dati che potrebbero far riferimento a vecchie informazioni ovvero *file* cancellati precedentemente.

[56] La previsione di effettuare più di una copia forense del dispositivo oggetto di analisi, oltre a fornire una maggior garanzia riguardo ad eventuali danneggiamenti accidentali dell'elemento probatorio, viene indicata dalla quasi totalità delle *best practices*, in particolare quelle prodotte a scopi investigativi.

specifici per l'analisi forense che garantiscono una buona affidabilità in termini di analisi e di reportistica finale, al fine di una migliore presentazione dei risultati ottenuti.

La scelta del *software* da utilizzare potrà essere lasciata al singolo analista in quanto l'utilizzo di strumenti differenti non pregiudica a priori la prova ma, eventualmente, potrà fornire risultati migliori o peggiori anche se certamente non differenti dal dato oggettivo individuabile sull'evidenza stessa.

E' fuori dubbio come, propedeutica all'attività di analisi dell'evidenza, possa essere necessaria una profilazione dell'utilizzatore del dispositivo oggetto di indagine.

Il profilo dell'utente, sia esso autore del reato, vittima o soggetto in qualsiasi misura interessato al fatto investigato, permetterà di fornire un più completo ed esaustivo esame dell'evidenza contestualizzandola in maniera puntuale all'interno dell'indagine stessa.

Conoscere le abitudini, il livello di competenze informatiche, le caratteristiche del soggetto, permetterà una più corretta e quantomai completa correlazione degli elementi anche non di natura digitale in possesso agli investigatori, al fine di poter addivenire ad un quadro ampio ed esaustivo del fatto investigato.

La fase documentale rappresenta la conclusione di tutto il processo legato all'acquisizione della prova digitale in quanto fissa l'intero operato degli investigatori, dall'individuazione della traccia sino al momento del suo esame e della presentazione delle conclusioni.

Tipicamente l'operatore di P.G. (ma anche il C.T. o il Perito) dovrà produrre una dettagliata documentazione relativa a tutte le operazioni effettuate sulla prova acquisita. La documentazione dovrà presentare un riepilogo descrittivo del dispositivo sottoposto a sequestro, nonché una relazione concernente tutte le attività svolte.

La relazione dovrà essere chiara e dovrà fornire nel dettaglio tutte le evidenze rilevate. Potrà essere correlata da documentazione fotografica e da una puntuale reportistica degli elementi presenti all'interno del dispositivo.

Buona norma sarebbe quella di evidenziare, in sede di documentazione finale, le caratteristiche delle singole evidenze rilevate e ritenute utili alle indagini al fine di fornire un quadro il più completo possibile[57].

Il processo di documentazione risulta quantomai fondamentale per garantire una corretta gestione della catena di custodia (*chain of custody*) dei reperti.

Per *chain of custody* si intendono tutte quelle operazioni, opportunamente documentate e dettagliate in ordine cronologico, che definiscono quando, come, dove e a quale scopo un reperto viene gestito (rinvenuto, repertato, depositato, trasmesso ad altri organi od uffici, acquisito, analizzato….).

Una corretta gestione del reperto contempla tutte quelle procedure atte a documentarne la raccolta, il trasporto, la sua corretta conservazione e l'analisi. Tali procedure hanno lo scopo di garantire che l'autenticità e l'integrità di quel reperto sia stata mantenuta in ogni fase, dalla sua

[57] Risulta importante, al fine di fornire un contesto spazio temporale, evidenziare i riferimenti temporali di memorizzazione e di utilizzo del dispositivo ovvero dei singoli file ritenuti utili alle indagini. Così come appare evidente rilevare se i dati riportati fossero presenti in aree allocate o cancellate, ovvero in cartelle temporanee o create dall'utilizzatore del sistema.

individuazione alla presentazione nelle aule di Tribunale.

Si deve tenere in considerazione che nel momento in cui un oggetto fisico o un dato diventa rilevante al fine di un'indagine viene considerato reperto e acquisisce uno *status* di particolare importanza in tutto l'*iter* probatorio prima e giudiziario dopo.

Il primo documento legato ad una corretta gestione della catena di custodia deve necessariamente nascere dal sopralluogo e dal suo relativo sequestro.

In particolare il codice di rito contempla l'obbligo di verbalizzare sia le attività del sopralluogo che quelle di sequestro[58].

I primi documenti legati alla catena di custodia di un reperto, così come espressamente prescritto dalla normativa vigente, sono quindi i verbali. Le modalità di loro redazione vengono individuate nel titolo III del libro II del Codice di Procedura Penale[59] dove compare la previsione della corretta indicazione delle circostanze di tempo e di luogo, delle motivazioni, con riferimento anche ad eventuali deleghe dall'Autorità Giudiziaria per cui si è reso necessario quel particolare atto, delle modalità operative utilizzate, oltre ovviamente alla menzione di tutte le persone intervenute.

La gestione dei reperti riveste un ruolo estremamente importante nelle attività di polizia giudiziaria, ma assume maggior rilievo quando i reperti per loro tipicità possono essere soggetti ad alterazione.

Come si è avuto modo di evidenziare, la prova informatica presenta le caratteristiche di estrema labilità, al pari dei reperti chimico-biologico che per loro natura sono facilmente deteriorabili; si aggiunga anche che il dato digitale potrebbe essere soggetto a modificabilità in ragione del supporto su cui è memorizzato. Bisognerà perciò porre una cura maggiore proprio in funzione della tipologia di elemento che si è sottoposto a repertazione.

Le migliori pratiche di *digital forensics* evidenziano e rimarcano l'importanza di una buona gestione della prova dal primo momento in cui questa viene individuata al fine di poter concretamente conoscere, istante per istante, dove si trovi il reperto acquisito e quali attività siano state effettuate su quel reperto.

La gestione della prova non si esaurisce però nella mera redazione di documentazione tecnico-giuridica ma deve prevedere una serie di procedure da attuare al fine di comprovare che tutti i supporti informatici sequestrati ed i dati ivi contenuti, sottoposti ad analisi, siano stati preservati ed adeguatamente protetti da danneggiamenti o da possibili alterazioni durante tutta l'attività investigativa.

La sola documentazione dunque non è sufficiente, occorre mettere in atto procedure che ne garantiscano una corretta gestione, utilizzando ad esempio appositi contenitori o buste antistatiche per i reperti digitali, depositando i corpi di reato digitali presso archivi che garantiscano condizioni di temperatura ed umidità costanti, privi di luce naturale ed adeguatamente schermati dal punto di

[58] Il Titolo IV del Libro V (artt. 347 e ss. C.P.P.) del codice di procedura penale individua le attività della Polizia Giudiziaria, prescrivendo oltre all'obbligo di riferire la notizia di reato, anche le modalità di assicurazione della fonte di prova, indicando altresì gli strumenti atti all'individuazione, alla ricerca e alla repertazione della stessa.

[59] Il titolo III del libro II, documentazione degli atti (Artt. 134 e ss. C.P.P.) fornisce le modalità di documentazione, il contenuto, la forma e le caratteristiche che devono avere gli atti redatti dalla Polizia Giudiziaria o dal P.M.

vista elettromagnetico[60]. Tali archivi dovrebbero altresì prevedere sistemi di protezione fisici ad accesso condizionato, con registrazione di ogni singola apertura. Il personale che interagisce con i reperti dovrà indossare appositi dispositivi antistatici, utilizzando strumentazione idonea nel momento in cui il reperto dovrà essere aperto per un successivo esame[61].

La normativa vigente si limita a prescrivere i casi e i modi entro cui si potrà acquisire o repertare una evidenza, documentandone la storia e prevedendo la redazione di verbali ogni qualvolta il reperto sia consegnato all'Ufficio Corpi di Reato del Tribunale, a un perito a un C.T., ovvero ad altro organo competente per le indagini tecnico-informatiche.

Il nostro ordinamento però non detta adeguate prescrizioni al fine di evitare ogni possibile alterazione, ovvero non entra nello specifico fornendo delle procedure da adottare nel momento in cui si debba gestire una evidenza digitale.

Altrove, in modo particolare negli Stati Uniti, o comunque in quasi tutti i paesi ove vige l'ordinamento di *common law*, la catena di custodia è uno *standard de facto*, messo in atto e rispettato dalle *law enforcement* come dalle agenzie federali di sicurezza.

In questi casi il rispetto delle procedure e l'agire secondo una metodologia comprovata sono alla base per una corretta gestione della prova e per il suo utilizzo in un procedimento.

Non seguire le procedure comunemente riconosciute pregiudica infatti quel reperto come elemento probatorio, inficiandone dunque la sua utilizzabilità.

La catena di custodia garantisce una continuità probatoria attraverso la possibilità di tenere traccia delle fasi di individuazione, acquisizione ed analisi, mediante la produzione di adeguata reportistica con differenti livelli di dettaglio. Viene dunque garantita la protezione delle prove, indicando tutti i soggetti che vi hanno accesso e le ragioni per cui tali soggetti hanno in qualsiasi misura interagito con il reperto.

Il *Computer Security Resource Center*[62] del NIST individua nella catena di custodia quel processo che tiene traccia dei movimenti delle fonti di prova durante le fasi di repertamento ed analisi ed altresì ne garantisce la salvaguardia attraverso una dettagliata documentazione che riporti, tra le altre informazioni, l'identità di ogni persona che ha trattato il supporto, la data e l'ora del repertamento o del trasferimento delle *digital evidence*s, con annessa motivazione.

Le procedure da adottare per una corretta gestione della catena di custodia devono essere estremamente semplici e devono contemplare sia la documentazione da redigere, sia le necessarie procedure da adottare per una corretta gestione della prova al fine di non danneggiarla. Questo non solo assicura l'integrità della prova, ma ne

[60] E' notorio come le cariche elettrostatiche o forti campi elettromagnetici possano interagire con i dati contenuti all'interno di tutti quei dispositivi di memorizzazione di tipo *read-write*, come ad esempio *Hard disk*, *floppy disk*, *pen drive*, memorie allo stato solido, memorie ad accesso casuale (RAM, ROM) etc. I soli dispositivi apparentemente non influenzabili da campi elettromagnetici sono i dispositivi ottici quali CD-ROM o DVD-ROM, etc., che comunque possono essere soggetti a degrado in particolare se vengono a contatto con sostanze solventi o composti solforosi.

[61] L'uso di bracciali antistatici è opportuno ogni qual volta si viene a contatto con dispositivi elettronici. Tali dispositivi permettono di scaricare eventuali cariche elettrostatiche dell'operatore, al fine di evitare ogni possibile danneggiamento dell'hardware sottoposto ad analisi.

[62] http://csrc.nist.gov/index.html (documento verificato in ultimo in data 15/10/2013).

rende difficile anche la contestazione dinanzi ad un giudice.

Un documento base da redigere per una corretta gestione della catena di custodia dovrebbe rispondere a determinati quesiti e conservare informazioni sull'identità degli operatori preposti al sequestro, su cosa è stato repertato e come è stato sottoposto a sequestro, dove erano posizionati i supporti/sistemi informatici, come vengono conservate e protette le evidenze e fornire informazioni anche sul personale tecnico che può disporre dei supporti per sottoporli alle analisi del caso. Tutta la documentazione dovrebbe inoltre essere conservata e posta al sicuro anche per eventuali verifiche *in itinere*.

4.1 Le differenti tipologie di intervento in ambito di *computer forensics*.

Al fine di fornire un quadro puntuale dell'intervento sulla scena del crimine digitale, è bene a questo punto indicare quali possano essere i possibili scenari e le tipologie di attività da eseguirsi nell'ambito della *digital forensics*.

Tipicamente l'intervento dell'investigatore deve differire in funzione dei dispositivi che dovrà acquisire ed anche delle situazioni operative che dovrà volta per volta affrontare.

La disamina delle tipologie di intervento di seguito riportata, che non vuole e non può essere esaustiva, ha comunque lo scopo di evidenziare e raggruppare in macro aree operative la maggior parte delle metodiche che più di frequente si presentano nella prassi quotidiana.

L'analisi *post mortem* è sicuramente la più frequente e forse quella maggiormente codificata a livello di migliori pratiche.

E' l'attività tipica dell'analista, effettuata in laboratorio, con le necessarie tempistiche e risorse tecniche che vengono richieste a un esame completo dell'evidenza informatica.

Essa fa riferimento all'analisi di un dispositivo spento o meglio privo di alimentazione, sia essa fornita attraverso la rete o anche attraverso accumulatori o batterie. Tale analisi, al fine di garantire l'assoluta ripetibilità dell'atto, deve ovviamente essere eseguita sulla copia del dispositivo.

L'analista, a seguito della produzione della copia lavoro dell'evidenza, acquisita attraverso le procedure precedentemente indicate al fine di assicurare una copia *bit-stream* del dispositivo, dovrà procedere alla verifica e al confronto dell'*hash* prodotto sul supporto originale in sede di repertazione con l'*hash* della sua copia, solo successivamente potrà proseguire con l'esame dei dati.

Con *live forensics analysis* invece si vuole indicare un'approccio estremamente delicato e spesso sconsigliato se non si posseggono le necessarie competenze tecniche.

Consiste in un'analisi preliminare del dispositivo durante la sua piena funzionalità, qualora non sia possibile procedere a repertamento e successiva analisi *post mortem* ovvero quando risulti necessario estrarre alcuni dati su un dispositivo il cui funzionamento non può essere interrotto[63].

Tipicamente viene posta in essere dagli operatori di P.G. o da Consulenti Tecnici o Ausiliari, nelle

[63] L'intervento dell'investigatore in ambito informatico, come indicato anche nelle più comuni *best practices* (vedasi *infra*), deve sempre tenere in considerazione l'operatività dei cosiddetti *mission critical device*, ovvero tutti quei dispositivi che per loro natura hanno una funzione specifica e critica e l'interruzione del loro funzionamento potrebbe arrecare gravi danni al sistema stesso, alle persone o alle cose (ad esempio, sistemi di controllo erogazione energia, sistemi di controllo sul trasporto pubblico, sistemi di

more dell'esecuzione di ispezioni o perquisizioni domiciliari, al fine di evidenziare elementi utili e procedere a un successivo sequestro.

Il recepimento della Convenzione di Budapest sui *cybercrimes* ha espressamente fornito agli Ufficiali e Agenti di Polizia Giudiziaria la possibilità di estendere l'ispezione e la perquisizione anche all'interno di sistemi informatici e telematici, attraverso i novellati artt. 244 e 247 c.p.p., ponendo come obbligo normativo l'adozione di misure tecniche idonee e dirette alla conservazione dei dati al fine di evitare eventuali alterazioni.

Tale tecnica, come accennato in precedenza, potrebbe trovare una sua positiva collocazione qualora si operi nell'ambito di indagini riferibili alla detenzione o divulgazione di materiale pedopornografico. In tale circostanza, l'accertamento della detenzione di un ingente quantitativo di materiale illecito o l'attualizzazione della sua divulgazione potrebbero divenire elementi utili e necessari all'applicazione della misura precautelare dell'arresto facoltativo in flagranza, *ex* art. 381 c.p.p.[64]

Potrebbe invece divenire indispensabile nel momento in cui risulti necessario acquisire dati o *file* presenti all'interno di sistemi informatici aziendali, attivi e funzionanti, quando l'interruzione di operatività potrebbe comportare irreparabili danni economici legati alla mancata fornitura di servizi. Si pensi ad esempio all'acquisizione di *file di log* presso società, ovvero alla ricerca di documenti contabili presenti all'interno di strutture anche molto grandi nelle quali sequestrare l'intera infrastruttura di calcolo sarebbe quantomeno inverosimile.

L'elemento chiave per la scelta della metodica tecnica da utilizzare per la raccolta degli elementi di prova è direttamente legato allo stato in cui il dispositivo viene rinvenuto, ove si presenti spento si potrà operare con le modalità dell'analisi *post mortem* in loco; in *stand-by*, acceso e perfettamente funzionante, qualora non sia possibile o consigliabile arrestarne il funzionamento al fine di evitare la perdita irreparabile di elementi di prova, si dovrà procedere ad un'analisi *live*[65].

La criticità di tale intervento consiste nel dover operare direttamente sui dispositivi che successivamente potranno essere sottoposti al vincolo del sequestro penale.

Qualora si debba operare su dispositivi in esecuzione, le cautele da porre in essere saranno maggiori in quanto superiore potrebbe essere il rischio di alterare la prova[66].

In tali circostanze, per l'acquisizione probatoria, si dovrà fare riferimento al cosiddetto ordine di volatilità delle evidenze informatiche, così come proposto dall'RFC 3227[67] o dalla più recente ISO/IEC 27037.

gestione di apparecchiature mediche per terapia o diagnosi, etc.).

[64] Al riguardo si ricorda come al comma 2 pt. I-bis dell'art. 381 C.P.P. sia previsto esplicitamente l'arresto facoltativo in flagranza in relazione agli artt. 600 *ter* e *quater* c.p. ovvero per l'offerta, cessione o detenzione di materiale pornografico prodotto mediante l'utilizzo di minori degli anni diciotto.

[65] Un'analisi di tipo *live*, contempla un elevato livello di professionalità in quanto potrebbe essere estremamente difficoltoso acquisire elementi di prova evitando ogni possibile alterazione del sistema.

[66] Un dispositivo in esecuzione, istante per istante, muta il suo stato anche solo nei riferimenti temporali relativi all'esecuzione o accesso a file di sistema, analogamente un dispositivo acceso produce ed aggiorna continuamente i file di log, interagisce eventualmente con il mondo esterno se collegato a reti di trasmissione etc.

[67] Le RFC (*Request For Comments*) sono un insieme di documenti di riferimento per la Comunità Internet che

Nell'ambito delle RFC 3227, ovvero le *Guidelines for Evidence Collection and Archiving*, si individua un livello differente di volatilità per ogni singola tipologia di evidenza informatica[68].

Tipicamente, per eseguire una corretta analisi di tipo *Live*, si dovranno acquisire le evidenze seguendo un ben definito ordine di priorità: registri di sistema, memoria *cache*, memoria delle periferiche (es. tabelle di *routing, etc.*), processi in esecuzione, dischi rigidi, file di *log* remoto e dati di controllo rilevanti per il sistema in esame, configurazione fisica del sistema informatico, topologia della rete, *Floppy Disk*, CD/DVD Rom e altri supporti ottici.

Altra tipologia di intervento che, nel tempo, sta acquisendo una sempre maggior importanza risulta essere quella definita con il termine generale di *network forensics analysis*.

Con questa metodologia si intendono tutte quelle attività di acquisizione e corretta gestione delle evidenze digitali che transitano attraverso una rete di comunicazione informatica o telematica.

Tale approccio può spaziare dalle intercettazione di flussi telematici, così come previsto dal dispositivo di cui all'art. 266 *bis* del codice di rito[69], sino all'acquisizione probatoria del contenuto di pagine *web*, ovvero della documentazione memorizzata su sistemi *cloud*[70].

Per tale motivo le metodologie applicabili sono le più varie e complesse, ma comunque tutte tenderanno a una gestione dell'evidenza informatica seguendo i consolidati principi di una corretta conservazione dei dati al fine di garantirne la genuinità, la non ripudiabilità e la non alterabilità.

In ultimo si vuole fare accenno alla cosiddetta *mobile forensics analysis*, ovvero quella disciplina che ricerca le evidenze digitali all'interno di dispositivi mobili attraverso metodologie riconosciute e comprovate dell'analisi forense.

E' sicuramente la metodica con un maggior grado di sviluppo in quanto un dispositivo mobile, oltre alle funzioni di telefonia, presenta capacità di calcolo e di memorizzazione sempre più elevate. In questa metodica si possono far rientrare rientrare anche tutte quelle attività legate all'acquisizione e analisi di qualsiasi dispositivo mobile o trasportabile quali ad esempio i *tablet*, gli *e-book reader*, i navigatori gps, etc.

Attualmente non si può parlare per i dispositivi mobili e per i dispositivi *embedded* di vera e propria analisi forense e, a tale proposito, sarebbe più appropriato riferirsi ad analisi di tipo *forensically sound*[71].

descrivono, specificano, standardizzano e discutono la maggioranza delle norme, degli standard, delle tecnologie e protocolli legati a internet e alle reti in generale. Gli RFC sono mantenuti e gestiti dalla *Internet Society* e vagliati dalla IETF (*The Internet Engineering Task Force*) e loro funzione primaria è quella di fornire degli standard di riferimento per le tecnologie utilizzate sulla rete Internet.

[68] Le RFC 3227 possono essere consultate al seguente indirizzo internet: http://www.faqs.org/rfcs/rfc3227.html (documento verificato in ultimo in data 9/05/2011).

[69] Art. 266 *bis* C.P.P., Intercettazione di comunicazioni informatiche o telematiche.

[70] In termini estremamente generali con il termine *cloud computing* si definiscono tutte quelle risorse informatiche (sistemi o servizi) che sono distribuite sulla rete e dunque non più localizzate ed accessibili attraverso sistemi di comunicazione. Per un approfondimento sul tema si rimanda, *inter alia*, al documento "*The NIST definition of Cloud Computing*" prodotto dal NIST e rinvenibile all'indirizzo http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (documento verificato in ultimo in data 10/12/2013)

[71] In informatica, con il termine sistema *embedded* (generalmente tradotto in italiano con sistema immerso o incorporato) si identificano genericamente tutti quei

Tali dispositivi presentando capacità computazionali non permettono in linea generale di effettuare analisi di tipo *post mortem*. Infatti per accedere ai dati al loro interno è spesso necessario interagire con specifici comandi senza avere la possibilità di accedere alla loro memoria quando questi non sono in funzione. Considerando i principi di non alterabilità e cristallizzazione della prova digitale, non risulta possibile dunque acquisire evidenze informatiche su tali dispositivi senza interagire, anche se in misura limitata, con il loro sistema operativo.

Le metodiche utilizzate per tali dispositivi tendono comunque a minimizzare le interazioni dell'operatore, anche se per tali attività, non essendo garantita la ripetibilità dell'atto, risulta evidente operare in base ai dettati dell'art. 360 c.p.p.

4.2 *Best practices*, cenni.

Il panorama internazionale negli ultimi tempi ha visto il proliferare di numerose linee guida, procedure e metodologie per approcciare la prova digitale nella maniera più corretta in funzione però di finalità e presupposti differenti in ragione dell'organismo, ente o associazione interessato alla produzione di tali buone pratiche.

Si possono infatti evidenziare protocolli sviluppati dalle agenzie di controllo, tesi a coniugare le necessità tecnico operative al quadro normativo di riferimento del singolo paese[72]; vi sono altresì procedure sviluppate a livello commerciale, al fine di normalizzare la gestione degli incidenti informatici a livello organizzativo imprenditoriale; esistono anche *standard* di matrice più propriamente tecnica, sviluppati da organismi di standardizzazione nazionale ed internazionale[73], che hanno lo scopo di fornire procedure tecniche universalmente riconosciute ed applicabili a prescindere del contesto normativo della singola nazione e in ultimo protocolli elaborati da associazioni di categoria[74], che hanno la finalità di fornire agli associati, generalmente personale altamente qualificato delle forze di

sistemi elettronici di elaborazione a microprocessore progettati appositamente per una determinata applicazione (*special purpose*) ovvero non riprogrammabili dall'utente per altri scopi, spesso con una piattaforma hardware *ad hoc*, integrati nel sistema che controllano e in grado di gestirne tutte o parte delle funzionalità. In questa area si collocano sistemi di svariate tipologie e dimensioni, in relazione al tipo di microprocessore, al sistema operativo, e alla complessità del *software* che può variare da poche centinaia di *byte* a parecchi *megabyte* di codice.

[72] Si evidenziano ad esempio i protocolli elaborati dal *Departement of Homeland Security* in collaborazione con *United State Secret Service*, denominati *Best Practices for Seizing Electonic Evidence*, vedasi *infra;* ma anche le *best practices* prodotte dall'anglosassone A.C.P.O. (*Association of Chief Police Officer*), denominate *Good Practice Guide for Digital Evidence*, reperibili in rete all'indirizzo http://library.npia.police.uk/docs/acpo/digital-evidence-2012.pdf (documento verificato in ultimo in data 12/12/2013).

[73] Corre l'obbligo di soffermarsi sulla recentissima approvazione e pubblicazione della norma ISO/IEC 27037 avente ad oggetto "*Guidelines for identification, collection an/or acquisition and preservation of digital evidence*". Tale norma, destinata a divenire standard *de facto*, si colloca tra quelle della serie ISO/IEC 27000 e rappresenta linee guida cui non è associata una specifica certificazione. La norma fornisce una metodologia da applicare nei processi di ricognizione, identificazione, catalogazione, acquisizione e conservazione dell'evidenza digitale, sia in ambito aziendale che istituzionale o processuale; non riguardando però le successive fasi di analisi e presentazione delle risultanze, nonché la successiva eliminazione degli elementi o informazioni acquisiti. Non presenta specifici riferimenti a normative statuali ma, tra i primari obiettivi di tali linee guida vi è quello di fornire procedure standardizzate per un corretto interscambio delle evidenze tra ordinamenti differenti. La norma ha un ambito di applicazione prettamente tecnico ed è destinata a operatori qualificati che intervengo sulla scena del crimine e che devono interagire con evidenze digitali .

[74] Si citano a titolo di esempio: IISFA International Information System Computer association, DFA Digital Forensics Affociation, IACIS Iternational Association of Computer Specialists.

polizia, accademici o ricercatori e consulenti privati, una certificazione in merito alle metodiche proposte, oltre che promuovere, attraverso il loro codice di condotta, una procedura comune e condivisa in ragione di elevate competenze tecniche e del contesto giuridico nazionale di appartenenza[75].

A prescindere dalle finalità e dall'applicabilità delle singole linee guida, il comune contesto tecnico operativo comporta ovviamente elementi di vicinanza nelle singole procedure, che possono essere riassunti nell'applicazione del metodo scientifico come approccio principale alle evidenze informatiche, con un diretto rimando alla ripetibilità, riproducibilità e non invasività delle operazioni compiute in ambito di *first response*.

A corollario di ogni procedura riconosciuta a livello internazionale vi è la necessità di predisporre una pedissequa documentazione finalizzata a garantire la tracciabilità e la catena di custodia delle prove digitali durante tutto il processo di gestione e presentazione delle evidenze stesse. Nello specifico, caratteristica della quasi totalità dei protocolli è quella di definire primariamente i compiti e le mansioni dei soggetti che dovranno approcciarsi all'evidenza informatica nelle varie fasi, dal primo intervento, all'attività più specialistica di sopralluogo, sino all'analisi stessa[76].

Molto risalto viene dato all'importanza di una preventiva preparazione della strumentazione necessaria e all'analisi delle informazioni in possesso, al fine di definire e coordinare le strategie più opportune nel corso dell'intervento. Il *briefing*, attività essenziale e prodromica nelle attività tecniche e, a maggior ragione, in tutte le operazioni di polizia, dovrà essere svolto con minuzia e attenzione, analizzando ogni possibile scenario.

La tipica attività di primo intervento spesso non coinvolge direttamente reparti specialistici: gli operatori "comuni" dovranno dunque aver cura di preparare, oltre alla dotazione standard a disposizione per l'espletamento dei servizi istituzionali, anche specifico materiale che potrebbe essere utile nel caso si debba intervenire in un contesto che preveda l'eventualità di repertare evidenze digitali.

Elemento riconducibile a tutti i protocolli, in particolare quelli prodotti a scopi investigativi o giudiziari, è la particolare attenzione che si deve riporre alla sicurezza degli operatori e al personale presente sulla scena, oltre che alla sicurezza e alla delimitazione del teatro operativo.

Risulta necessario limitare al minimo l'impatto e l'interazione con gli elementi presenti all'interno del luogo di intervento, non alterando lo stato delle cose e isolando l'area utilizzando, a tal fine, procedure e strumentazioni non invasive.

Molto risalto viene dato anche alla valutazione delle tipologie di sistemi informativi su cui si deve operare, anche in funzione delle finalità e dello scopo dell'intervento[77].

---

[75] Per una puntuale analisi sulle differenti tipologie di linee guida nel contesto internazionale si rimanda a D. La Muscatella, "La genesi della prova digitale: analisi prospettica dell'informatica forense nel processo penale", in *Ciberspazio e Diritto*, n. 2, 2012, pp. 385-416.

[76] Si segnala, a titolo esemplificativo, come la norma ISO/IEC 27037 definisca il "chi fa cosa" in maniera pedissequa, individuando specifiche figure in funzione delle specifiche competenze e dei momenti di interazione con l'evidenza stessa, ovvero: *Digital Evidence First Responder (DEFR), Digital Evidence Specialist (DES), Incident Responder Specialist, Forensics Laboratory Manager.*

[77] Durante il primo intervento sulla scena, quando si hanno di fronte strumentazioni altamente tecnologiche, non si può prescindere dalle funzionalità di queste e

Vengono altresì fornite indicazioni in merito alla valutazione, nell'acquisizione degli elementi, della presenza di dati o informazioni di terze parti non direttamente coinvolte nella vicenda, ma anche alla stima della priorità di acquisizione delle evidenze (*triage*) in funzione della maggior o minor volatilità delle stesse[78].

In ultimo, regole a carattere generale da tener maggiormente in considerazione, sono quelle di evitare l'accensione di un dispositivo rinvenuto spento ed analogamente valutare lo spegnimento di un dispositivo rinvenuto acceso prima di aver ultimato l'acquisizione di tutte le evidenze in base all'ordine di priorità e prima di aver fatto una corretta valutazione sulle procedure da utilizzare per lo spegnimento stesso del dispositivo[79].

Ultima ma imprescindibile regola comune a tutti i protocolli è quella che prevede che, in caso di dubbi o di non conoscenza del sistema, sia sempre bene sospendere ogni attività, delimitare l'area e contattare uno specialista, che potrà intervenire direttamente ovvero fornire le necessarie informazioni per una corretta repertazione.

5. Buone pratiche e migliori pratiche. Riflessioni sulla realtà italiana.

Non molti anni sono passati da quando la *computer forensics* si è affacciata timidamente nelle vicende giudiziarie nazionali, tale disciplina però nel tempo si è imposta come valore aggiunto prima e come attività imprescindibile ora anche in

prima di operare bisogna sempre tenere in considerazione quale impatto potrebbe avere sul sistema informatico una qualsiasi azione. Estrema attezione dovrà essere posta ai *mission critical device* e alla tutela della *business continuity*. Si pensi ad esempio a un intervento su sistemi informatici che gestiscono l'operatività di grandi aziende, di enti o di grosse società di servizi, dove interromperne il funzonamento potrebbe comportare gravi danni economici; si pensi altresì quando risulti necessario interagire con dispositivi medici estremamente complessi (apparati per la tomografia computerizzata o per radioterapia) dove un minimo errore potrebbe comprometterne il corretto funzionamento con gravi ripercusioni sulla salute dei pazienti.

[78] Come già indicato, le evidenze digitali pur essendo estremamente fragili, presentano un differente grado di volatilità in funzione del supporto o del sistema in cui sono presenti. Si richiama in proposito quanto prescritto dalle RFC 3227, che in relazione all'ordine di volatilità delle evidenze fornisce un elenco di priorità di intervento, vedasi *supra*.

[79] Nel caso in cui venga rinvenuto un elaboratore acceso viene indicato come togliere l'alimentazione agendo sulla presa di corrente, invece che effettuare le comuni procedure di spegnimento del sistema, risulti essere la soluzione meno distruttiva in termini di conservazione della prova informatica. E' indubbio come una operazione così drastica possa rilevare dubbi sulla effettiva correttezza metodologica, bisogna però considerare, in estrema *ratio*, che la priorità ultima non è preservare il sistema nel suo complesso ma l'evidenza informatica nello specifico. Togliere la spina lato elaboratore e non lato presa a muro produce un immediato spegnimento della macchina con conseguente congelamento di ogni eventuale attività, preservando eventuali informazioni presenti in *cache non volatili* o nei *file* temporanei. Esistono varie teorie che indicano perché bisognerebbe agire staccando l'alimentazione lato computer e non lato presa a muro, alcune non del tutto scientificamente corrette. La spiegazione più logica di tale operazione è riferibile al fatto che, se l'elaboratore risulta collegato ad un sistema UPS (gruppo di continuità – apparato che si attiva nel momento in cui si verifica un calo di tensione, ed ha lo scopo di fornire alimentazione al sistema per un tempo variabile in funzione delle caratteristiche dell'UPS stesso) che ne garantisce l'operatività in assenza temporanea di tensione, agendo lato presa a muro non si spegnerà l'elaboratore poiché, in automatico, verrebbe erogata corrente dal sistema UPS. Togliendo il cavo lato *computer* questa eventualità non si potrebbe verificare, consentendo uno spegnimento immediato della macchina. In ultimo le valutazioni in ordine allo spegnimento del sistema, utilizzando le "normali procedure", sono riferibili al fatto che esistono applicativi specifici di *antiforensics* (ovvero tecniche per alterare o rendere inutilizzabili in maniera dolosa le evidenze digitali) che consentono, previo l'invio di comandi anche da remoto, una distruzione pressoché totale dei dati memorizzati, tali strumenti possono intervenire anche nel caso in cui non si seguano procedure specifiche e non conoscibili a priori per arrestare l'elaboratore (*i.e.* tener premuto una specifica sequenza di tasti prima di effettuare la procedura di arresto). Esistono infatti applicativi che installati rimangono silenti ed invisibili all'operatore e possono essere impostati in modo da distruggere determinate porzioni di disco nel momento in cui si effettuano le normali procedure di spegnimento.

giudizi non direttamente collegati ai reati informatici classici.

Il punto di forza può essere individuato nello stretto connubio esistente tra scienza e attività investigativa: la scientificità assunta nella gestione delle evidenze ha l'effetto di rafforzare il loro valore probatorio in sede dibattimentale.

Fondamentale nell'acquisizione probatoria della prova informatica è il metodo scientifico applicato alle fonti di prova che trova una sua collocazione nello sviluppo di protocolli operativi avallati dalla comunità scientifica.

Come già accennato, in Italia non esistono *standard* o metodiche operative di riferimento e prodotte a livello nazionale con lo scopo di operare nella maniera più corretta sull'evidenza informatica. I reparti specializzati delle forze di polizia operano fondamentalmente seguendo le procedure internazionali, senza per altro avere un punto di riferimento nella realtà nazionale.

Si cita, tra tutte, l'esperienza della Polizia Postale e delle Comunicazioni, specialità della Polizia di Stato al cui vertice con Decreto Interministeriale del 19 gennaio 1999 è stato istiuito il Servizio Polizia Postale e delle Comunicazioni, indicato quale organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi di telecomunicazioni[80].

Tale Reparto, altamente specializzato in materia di *computer crimes* e *computer related crimes*, opera da tempo utilizzando metodologie e protocolli internazionalmente riconosciuti, senza però disporre di proprie buone pratiche o di un proprio protocollo operativo, se non individuabile attraverso alcune circolari ad uso interno, emanate dal Servizio, in ordine a particolari attività investigative ovvero a specifiche tipologie di indagini[81].

Anche se apparentemente tale lacuna potrebbe essere letta con una connotazione negativa, ad onor del vero appare essere una strategia vincente che colloca la Polizia delle Comunicazioni in un contesto di collaborazione internazionale, attribuendole elevata professionalità e scientificità nell'operare in realtà ad alto impatto tecnologico.

Da tempo infatti il Servizio Polizia Postale e delle Comunicazioni ha attivato programmi di formazione altamente specializzanti per i suoi operatori. A tale riguardo si vuole rimarcare come gli ufficiali e gli agenti di P.G. in forza presso la Specialità della Polizia di Stato devono necessariamente frequentare un corso di specializzazione per i servizi di Polizia Postale e delle Comunicazioni che prevede lezioni teorico-pratiche inerenti le problematiche giuridiche e tecnico informatiche legate al mondo delle telecomunicazioni e delle nuove tecnologie. La formazione per gli appartenenti alla Polizia delle Comunicazioni è comunque costante: ogni anno sono previste lezioni teorico-pratiche di aggiornamento professionale nelle materie di competenza oltre a percorsi formativi altamente

[80] Il Servizio Polizia Postale e delle Comunicazioni, con sede a Roma, coordina l'attività dei 20 Compartimenti, localizzati nei capoluoghi di regione. I Compartimenti hanno competenza regionale e coordinano le 76 Sezioni all'interno del proprio territorio di competenza. La Polizia Postale e delle Comunicazioni ha competenze in materia di controllo e repressione degli illeciti penali ed amministrativi nel settore delle comunicazioni in genere, incluse ovviamente le attività di prevenzione e contrasto in ordine ai *computer crimes* e *computer related crimes.*

[81] In particolare, anche in funzione delle specifiche attività investigative, i protocolli maggiormente utilizzati sono quelli elaborati dal *Departement of Homeland Security* in collaborazione con *United State Secret Service*, ma anche le *best practices* prodotte dall'anglosassone A.C.P.O.

qualificanti per gli appartenenti ai ruoli più operativi[82].

Il Servizio Polizia Postale e delle Comunicazioni è attivo altresì nel promuovere un costante interscambio esperienziale con agenzie governative europee ed americane[83]. L'assenza di procedure nazionali codificate potrebbe dunque essere letta come punto di forza e non di debolezza, poiché si rimanda alla più ampia comunità scentifica internazionale la validazione delle necessarie metodiche di approccio alle evidenze digitali.

Considerando che gli strumenti giuridici a disposizione della polizia giudiziaria stabiliscono il solo principio finalistico di non alterabilità e corretta conservazione della prova digitale non entrando dunque nel merito dell'operatività spicciola, sarebbe comunque opportuno nella realtà italiana individuare un organismo che stabilisca, in maniera più snella e veloce rispetto a quanto potrebbe richiedere una costante produzione normativa, procedure comuni anche in relazione alle metodologie internazionali. Siffatte procedure, avallate dunque a livello nazionale, potrebbero divenire punto di riferimento per tutti quegli operatori coinvolti in attività di *computer forensics* e non solo quelli applicati nei reparti specialistici[84]. Tale organismo potrebbe altresì approvare o certificare quelle procedure già consolidate a livello internazionale, al fine di ottenere parametri certi da applicare nel contesto nazionale, riconoscibili e condivisi anche nelle varie sedi e gradi di giudizio.

Si deve però considerare come un protocollo specificatamente tecnico orientato ad una corretta gestione dell'evidenza informatica necessiti di importanti competenze da parte degli organi interessati, siano essi istituzionali o privati. Tali capacità, non sempre facili da reperire, obbligherebbero in primo luogo una formazione altamente qualificata per tutti gli operatori, anche quelli impegnati nel primo intervento, fornendo competenze non sempre necessarie per l'espletamento degli incarichi quotidiani a scapito di un dispendio enorme di risorse riservabili per una continua e necessaria formazione specialistica.

Un esperto forense in ambito informatico deve possedere infatti competenze giuridiche e tecnico-scientifiche che richiedono un continuo e costante aggiornamento, al pari della continua e costante evoluzione tecnologica e della produzione normativa in materia.

Una così capillare e regolare formazione non potrà mai essere rivolta a tutto il personale operativo delle forze di polizia, in quanto

[82] Si cita tra i tanti momenti formativi ad alta specializzazione il corso semestrale di aggiornamento professionale sulla *computer forensics* organizzato in collaborazione con la Scuola di Scienze e Tecnologie dell'Università di Camerino.

[83] Il Servizio è punto di contatto internazionale per le emergenze a carattere informatico ed è presente in numerosi gruppi di lavoro internazionali quali ad esempio l'Electronic Crime Task Force (ECTF), *European Financial Coalition* (EFC) ed è parte del network di polizie denominato Virtual Global Task Force (VGT). Si veda al proposito http://www.commissariatodips.it/profilo/collaborazione-internazionale.html (documento verificato in ultimo in data 10/12/2013).

[84] Come verrà analizzato nel prosieguo, a livello internazionale l'Organizzazione Internazionale per la Normazione (ISO) all'interno degli standard ISO/IEC 27000 ha proposto la norma ISO/IEC 27037 "*Guidelines for identification, collection, acquisition, and preservation of digital evidence"* che fornisce linee guida per la gestione (*handling*) della prova informatica. Tale norma, approvata e pubblicata nell'ottobre 2012 non prevede una specifica certificazione ma di fatto fornisce linee guida all'interno di uno standard ed una certificazione più articolata (ISO/IEC 27000) relativo ai Sistemi di Gestione della Sicurezza delle Informazioni (SGSI).

comporterebbe un dispendio di risorse non commisurato alle reali necessità del quotidiano.

Per tali motivazioni potrebbe essere sensato sviluppare una doppia metodologia operativa: una prima correlata al concetto del "massimizzare la perdita minore" o di "*least worst"*, una seconda invece specifica per gli operatori dei reparti specialistici[85].

Mutuando il criterio del *minmax* dalla teoria dei giochi[86] e riferendosi alla definizione di strategia ottimale, il protocollo operativo rivolto al personale non specializzato dovrà essere orientato a garantire l'inalterabilità dell'elemento probatorio in funzione delle risorse disponibili in una determinata circostanza. Si potrebbe dunque indicare che una "procedura normale standard" applicabile alla *computer forensics* potrebbe essere intesa come quella procedura che mira ad ottenere l'inalterabilità dell'elemento probatorio in funzione delle risorse disponibili, delle circostanze di tempo e di luogo e della necessità di operare in quel contesto senza poter attendere l'intervento di personale altamente specializzato[87].

Il protocollo operativo standard sarà indirizzato agli operatori di *first response,* ovvero a tutte quelle figure professionali che, per ragioni istituzionali, sono chiamate a individuare le fonti di prova e ad evitare che queste vengano irreparabilmente disperse e dovrà essere applicato in teatri operativi non complessi, per l'acquisizione di evidenze digitali comuni[88].

Un secondo protocollo più tecnico, orientato ad una completa e corretta procedura di gestione della prova, sarà sviluppato per il personale dei reparti specialistici o per i consulenti tecnici in possesso delle necessarie competenze, che dovranno intervenire qualora le realtà operative richiedessero un apporto specializzato.

Tali ipotesi, di fatto, non si discostano di molto da quanto avviene nella pratica quotidiana delle indagini tradizionali, infatti gli operatori impegnati nei servizi di controllo del territorio posseggono già una adeguata formazione che permette loro di gestire un primo intervento sulla scena del crimine. Tale conoscenza presuppone attività finalizzate alla circoscrizione del teatro operativo, all'acquisizione dei primi elementi e alla reperatazione probatoria di base, per poi lasciare il campo al personale di polizia scientifica, che dovrà condurre il più specifico ed accurato sopralluogo tecnico.

5.1 Il panorama internazionale.

L'approccio anglosassone o meglio ancora statunitense alla *digital forensics* da sempre si basa sulla produzione di procedure da somministrare agli operatori interessati alla raccolta degli elementi probatori, tale

[85] Il concetto che si vuole introdurre prende spunto dalla Teoria delle Decisioni e nello specifico dal cd. criterio del *minmax*. Tale teoria viene utilizzata per produrre modelli decisionali volti a minimizzare le perdite in situazioni a complessità variabile nel caso in cui si debba adottare una strategia operativa pur non conoscendo approfonditamente la realtà in cui si deve operare. Il criterio del *minmax* rientra nella più ampia Teoria dei Giochi. Per un approfondimento si rimanda a F.S. Hillier, G.J. Lieberman, *Introduzione alla ricerca operativa*, Franco Angeli, Milano, 1994, pp. 106 e ss.

[86] Per un approfondimento sulla teoria dei giochi si rimanda *inter alia* a F. Colombo, *Introduzione alla teoria dei giochi*, Carrocci, Roma, 2003.

[87] Un simile protocollo risulta per altro già presente e consolidato a livello internazionale. Si veda in proposito le citate *Best Pracitices for Seizing Electonic Evidence*, che di fatto prevedono principalmente procedure relative al primo intervento sulla scena da parte di operatori non appartenenti a reparti specializzati, vedasi *infra*.

[88] Si pensi ad esempio alla repertazione di *personal computer, laptop, hard disk* o dispositivi di memoria

orientamento non si discosta molto dalla metodologia utilizzata dalle varie forze di polizie ed agenzie governative impiegate in operazioni di ordine pubblico, primo soccorso ed attività di indagine di vario tipo.

Siffatta metodologia trova diretto riscontro nel mondo anglosassone in genere, sia nelle tipiche caratteristiche degli ordinamenti di *common law*, sia nella maggior attitudine a seguire regole precodificate per far fronte a situazioni a complessità variabile.

Tutto ciò si discosta molto dall'approccio di tipo "*a bricolage"* troppo spesso invocato nel vecchio continente, che sfrutta conoscenze pregresse o esperienze maturate al fine di risolvere situazioni nuove o con differente complessità[89].

Se l'approccio procedurale in ambito investigativo non sempre riscuote gli effetti voluti, in ambito di *computer science*, o meglio di acquisizione della *digital evidence*, diviene fondamentale, poiché in tale fase convergono aspetti tecnici, giuridici ed investigativi[90].

Il *Departemend of Homeland Security* americano e lo *United State Secret Service (USSS)*, da tempo, sono impegnati in un progetto comune per la produzione di linee guida utilizzabili nell'ambito dell'acquisizione della prova informatica.

Il progetto, denominato *Best Practices for Seizing Electronics Evidence*, ha prodotto una serie di protocolli operativi, pubblicati successivamente all'interno di un manuale in uso alle forze di polizia, ma di fatto, nella sua quasi totalità, di dominio pubblico, con lo scopo di fornire una conoscenza di base tecnica e giuridica sugli aspetti della corretta gestione della *digital evidence*[91].

Gli operatori devono essere in grado di intervenire sulle problematiche maggiormente frequenti, legate ad operazioni di polizia, che contemplino elementi ad alto impatto tecnologico.

Devono poter individuare i singoli dispositivi digitali, comprendere quali possano essere utili all'attività investigativa e possedere le necessarie competenze per poter operare direttamente, ovvero fare riferimento agli appartenenti alle squadre ECSAP (*Electronic Crime Special Agent Program*).

Un aspetto molto curato in tutte le *guidelines* sviluppate dalle numerose agenzie governative, associazioni o forze di polizia, è quello legato alla sicurezza dell'operatore (*officer safety*) e quindi alla preparazione dell'intervento o dell'operazione di polizia[92].

---

allo stato solido etc., dove utilizzando semplici accorgimenti si possono escludere eventi distruttivi.

[89] L'approccio al *bricolage* si basa sullo sfruttamento delle risorse a disposizione localmente e sulla ricombinazione intuitiva e "artistica" che si adatta alla situazione e alle circostanze del momento. Cfr. C. Ciborra, "From Thinking to Thinkering: The Grassroots of Strategic Information Systems", *The Information Society*, 8,4, pp. 297-309.

[90] L'attività investigativa non sempre può essere vincolata a procedure stringenti in quanto l'intuito e la capacità di *problem solving* rivestono un ruolo molto importante. L'aspetto procedurale (non inteso in termini giuridici ma pratici) determina il metodo da perseguire ma non può vincolare l'operato dell'investigatore.

[91] Il progetto, ormai giunto alla terza edizione, si presenta come una guida tascabile. E' reperibile anche sulla rete internet all'indirizzo: http://www.forwardedge2.com/pdf/bestpractices.pdf (documento verificato da ultimo il 18 maggio 2013).

[92] Come già evidenziato, le procedure proposte dall'USSS non sono le uniche presenti nel panorama americano, infatti si rilevano analoghe linee guida prodotte dal Dipartimento di Giustizia, dall'*International Association of Chief Police*, dall'FBI, etc. le procedure presenti si discostano di poco dal punto di vista tecnico, affrontano però in alcuni casi procedure differenti per quanto concerne l'aspetto legale della gestione della prova. Questo perché ogni agenzia opera in settori differenti con competenze diverse e normativa in alcuni casi speciale in funzione delle attività svolte.

Altro aspetto al quale si dà molto risalto fa riferimento alla dotazione personale o di squadra (*tecnical equipment*) per i singoli reparti impegnati in operazioni di *Search and Seizure.*

Vengono infatti indicati in maniera minuziosa quali siano gli strumenti necessari per una corretta gestione dell'intervento, puntualizzando che dovranno essere evitati tutti quegli strumenti che possano trasmettere, produrre o diffondere campi elettromagnetici o cariche elettrostatiche, al fine di evitare il danneggiamento dei reperti.

Nella guida dell'USSS vengono evidenziate le tipologie di intervento in funzione degli strumenti giuridici a disposizione, indicando procedure leggermente differenti nei diversi casi di operazioni del tipo *Arrest Warrant, Search Warrant, Knock and Talk,*etc. [93]

La parte prettamente tecnica operativa invece è molto simile in tutte le *guidelines* analizzate e fondamentalmente mira a protocolli per l'assicurazione della scena del crimine, l'isolamento dei *device* rinvenuti, la documentazione, la preservazione e l'assicurazione probatoria.

Vengono impartite disposizioni per la gestione di alcuni dei principali dispositivi che ipoteticamente possono essere presenti sulla scena, indicando la maniera migliore per repertare (*to collect*) le singole evidenze.

Punto comune a tutte le guide è l'estrema praticità e schematicità descrittiva: il manuale, che si presenta nelle tipiche dimensioni di una piccola agenda tascabile, dovrebbe essere presente nella dotazione personale del singolo operatore e prontamente utilizzabile con estrema facilità d'uso.

Le finalità di tale progetto e della maggior parte delle linee guida statunitensi analizzate è quella di formare l'operatore non specializzato al fine di fornire gli elementi base per la gestione delle evidenze digitali, rimandando per altro alle squadre di specialisti la gestione di situazioni complesse.

6. Riflessioni conclusive.

Negli ultimi anni la prova informatica ha assunto un ruolo sempre più importante nell'ambito delle investigazioni giudiziarie e, come giustamente evidenziato, *"l'introduzione delle tecnologie dell'informazione nel mondo criminale, anche se relativamente recente, ha avuto un'immediata propagazione a tutti i livelli, dal singolo alle organizzazioni più sofisticate"*[94].

La *computer forensics*, oltre a basarsi su precisi fondamenti scientifici, presenta connotazioni tipiche dell'attività investigativa, motivo per cui non può essere ricondotta a mera attività di supporto dell'attività di polizia giudiziaria.

L'analista forense delle evidenze digitali ha l'onere di fornire in maniera puntuale e con l'avallo del metodo scientifico una connotazione spazio temporale dell'evento investigato definendo fatti, confutando alibi, correlando elementi o accadimenti.

Di fondamentale importanza nell'analisi della *digital evidence* è la correlazione di fatti, elementi, indizi che, travalicando la mera disamina di stampo ingegneristico o peritale di un

[93] *Knock and Talk* fa riferimento all'attività tipica d'iniziativa dell'investigatore ed è finalizzata alla cosiddetta intervista investigativa (*Investigative interview*) ed alla raccolta probatoria preliminare.

[94] G. Marotta, "Tecnologie dell'Informazione e processi di Vittimizzazione", in *Rivista di Criminologia, Vittimologia e Sicurezza*, n. 2, 2012, p. 94.

elemento repertato, ne caratterizza la formazione di elementi probatori.

L'esempio più classico, esaminato nel corso di questa trattazione, è quello del biologo forense che, analizzando un frammento di codice genetico, può scientificamente dimostrare la presenza di un soggetto sulla scena del crimine; tale circostanza, nell'ambito del processo investigativo, dovrà essere correlata ad altri elementi, tipicamente acquisiti nell'attività d'indagine, al fine di ottenere una linea temporale che definisca *quando*, *come* e *perché* quel soggetto, quella traccia, quell'elemento fosse stato presente in quel determinato luogo.

In ambito digitale questa correlazione spetta invece all'investigatore informatico, che deve necessariamente interagire con il fatto investigato, assumendo elementi anche non di carattere informatico, esaminando le tracce, non per forza digitali e correlando gli aspetti assunti nelle evidenze acquisite.

Tali attività dovranno necessariamente essere compiute con perizia, scienza e coscienza, al fine di poter assumere l'elemento digitale come prova e proporla nelle opportune sedi giudiziarie.

La disamina del codice di rito ha permesso di rilevare le innovazioni presenti nella legge di ratifica della Convezione di Budapest sui *Cybercrimes*, introdotta nel nostro ordinamento con legge 18 marzo 2008, n. 48, che, novellando ed ampliando gli istituti giuridici deputati alla ricerca delle fonti di prova, ha introdotto nell'ordinamento nazionale i principi cardine della *computer forensics.*

La legge, seppur lacunosa nelle specifiche procedure tecniche da adottare, ha comunque affermato i principi fondamentali della conservazione, dell'integrità e della non alterabilità della prova informatica anche in situazioni emergenti, prevedendo l'applicazione di corrette procedure al fine di evitare l'alterazione dell'elemento digitale.

E' indubbio come l'investigatore moderno debba sempre più frequentemente confrontarsi con le nuove tecnologie al fine di poter fornire una risposta certa, precisa e minuziosa al fatto investigato. Per questo motivo, e per le caratteristiche dell'ambiente virtuale sembre più interconnesso con quello reale, dovrà operare in base a procedure codificate e non esclusivamente sulla scorta dell'intuito personale, dell'improvvisazione o dell'esperienza.

Tali elementi certamente necessari, fondamentali ed indispensabili all'attività investigativa, non rappresentano più condizioni sufficienti per un approccio moderno alle scienze criminali.

Gli apparati investigativi, dunque, dovranno sempre di più organizzare le proprie attività in maniera sinergica, prevedendo all'interno dei propri organici figure specializzate e altamentente preparate che possano fornire un contributo certo nella gestione di ambienti altamente tecnologici, dovranno altresì riconsiderare, dal punto di vista tecnico, anche i programmi addestrativi, inserendo nella didattica di base i rudimenti necessari affinché anche il singolo operatore possa gestire in maniera corretta le evidenze digitali.

Bibliografia.

- Agarwal A. *et al.*, "Systematic digital forensic investigation model", in *International Journal of Computer Science and Security (IJCSS)*, vol. 5, n. 1, 2011.
- Alharbi S., Weber-Jahnke J., Traore I., "The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature

Review", in *Information Security and Assurance*, 2011, pp. 87-100.
- Aterno S., Cajani F., Costabile G., Mattiucci M., Mazzaraco G., *Computer forensics e Indagini Digitali, Manuale tecnico giuridico e casi pratici*, Forlì, Experta, 2011.
- Bravo F., "Indagini informatiche e acquisizione della prova nel processo penale", in *Rivista di Criminologia, Vittimologia e Sicurezza*, 3/2009 – 1/2010 (numero doppio).
- Bravo F, *Criminalità economica e controllo sociale. Impresa etica e responsabilità ex d.lgs. 231/01*, Bologna, Clueb, 2010.
- Casey E., *Digital Evidence and Computer Crime Forensic Science, Computers, and the Internet*, Academic Press, Londra 2000.
- Cajani F., Costabile G. (a cura di), *Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea*, Experta, Forlì, 2011.
- Cajani F., "La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, ovvero: quello che le norme non dicono…", in *Ciberspazio e Diritto*, Vol. 11, n. 1, 2010.
- Costabile G., "Computer forensics e informatica investigativa alla luce della Legge n.48 del 2008", in *Ciberspazio e Diritto*, Vol. 11, n. 3, 2010.
- Forte D., "Le attività informatiche a supporto delle indagini giudiziarie", in *Rivista della Guardia di Finanza*, 2, 2000.
- Ghirardini A., Faggioli G., *Computer forensics*, Apogeo, Milano, 2007.
- Galdieri P., *Teoria e pratica nell'interpretazione del reato informatico*, Giuffrè, Milano, 1997.
- Henseler J., *Computer Crime and Computer forensics*, in *Encyclopedia of Forensic Science*, Academic Press, Londra, 2000.
- Hillier F.S., Lieberman G.J., *Introduzione alla ricerca operativa*, Franco Angeli, Milano, 1994.
- Ingletti V., *Diritto di polizia giudiziaria*, Laurus Robuffo, Roma, 2006.
- Intini A., Casto A.R., Scali D.A., *Investigazione di polizia giudiziaria, manuale delle tecniche investigative*, Laurus Robuffo, Roma, 2006.
- La Muscatella D., "La ricerca della prova digitale e la violazione delle best practices: un'attività investigativa complessa tra recenti riforme e principi consolidati", in *Ciberspazio e Diritto*, Vol. 12, n. 2, 2011.
- La Muscatella D., "La genesi della prova digitale: analisi prospettica dell'informatica forense nel processo penale", in *Ciberspazio e Diritto*, Vol. 13, n. 3, 2012.
- Luparia L., Ziccardi G., *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007.
- Luparia L. (a cura di), *Sistema penale e criminalità informatica*, Giuffrè, Milano, 2009.
- Maioli C., *Dar voce alle prove: elementi di Informatica forense*, in internet all'indirizzo : http://www.dm.unibo.it/~maioli/docs/fti_informatica_3009.doc
- Marotta G., "Tecnologie dell'Informazione e processi di Vittimizzazione", in *Rivista di Criminologia,Vittimologia e Sicurezza*, 2, 2012.
- Marturana F., Tacconi S., "A Machine Learning-based Triage methodology for automated categorization of digital media", in *Digital Investigation*, Vol. 9, 2013.
- Picozzi M., Intini A. (a cura di), *Scienze forensi. Teoria e prassi dell'investigazione scientifica*, Utet, Torino, 2009.
- Piccini M. L.,Vaciago G., *Computer crimes, Casi pratici e metodologie investigative dei reati informatici*, Moretti & Vitali, Bergamo, 2008.
- Robbins J., *An explanation of Computer forensics*, in internet all'indirizzo http://www.pivx.com/forensics
- Rosen R.A., *Forensics e frodi aziendali, intervento alla Giornata di studio A.I.E.A.*,Roma, 21 novembre 2001.
- Senor M. A., *Legge 18 marzo 2008, n. 48 di ratifica ed esecuzione della Convenzione di Budapest sulla criminalità informatica: modifiche al codice di procedura penale ed al D.Lgs. 196/03*,in *Altalex, Quotidiano scientifico di informazione giuridica*, in internet all'indirizzo: http://www.altalex.com/index.php?idnot=41576
- Tonini P., *Manuale di procedura penale*, Giuffrè, Milano, 2010.