UNIVERSITÀ DEGLI STUDI DI UDINE

CORSO DI LAUREA IN SCIENZE DEI SERVIZI GIURIDICI PUBBLICI E PRIVATI

TESI DI LAUREA IN LINEAMENTI DI INFORMATICA GIURIDICA

PROBLEMI DELLA *MOBILE FORENSICS* IN AMBITO PENALISTICO

Relatore: Prof. Aggr. Federico Costantini

Laureando: Roberto Demarchi

ANNO ACCADEMICO: 2014/2015

Sommario

INTRODUZIONE

Da qualche decennio a questa parte, dapprima i computer, poi i dispositivi digitali più vari, sono entrati a far parte in modo diffuso nell'uso quotidiano delle persone. Oggi i dispositivi più comuni sono rappresentati da *smartphone*, *tablet*, e *notebook*. Utilmente impiegati, per la loro versatilità e la molteplicità di funzioni, nell' attività lavorativa e nella normale vita quotidiana, sono anche inevitabile archivio di dati personali di chi li utilizza e, aspetto più delicato, degli individui con cui questi si relazionano. Non è un azzardo affermare che i dati in essi allocati forniscono indicazioni anche estremamente precise riguardo alle abitudini e agli stili di vita dei loro possessori. Traccia di queste informazioni, e delle potenziali condotte che esse rivelano, sono contenute sia nelle memorie elettroniche dei dispositivi sia nello spazio Internet o nei provider delle reti di comunicazione cellulari qualora questi dispositivi siano connessi alle reti telematiche e mobili. Il più delle volte questo avviene senza che l'utente ne sia consapevole[1]. Fonte di informazione possono essere per esempio i metadati[2] contenuti nelle foto fatte con uno *smartphone* (ora, data, localizzazione con *gps*) a cui si aggiungono le funzionalità messaggistiche testuali e multimediali che ripercorrono le nostre azioni di vita quotidiana.

Collegarsi con questi dispositivi ad Internet per la semplice ricerca di notizie o per l'utilizzo dei *social network* e la posta elettronica, fruire del *cloud* come *storage*[3] o della telefonia *mobile* (*smartphone*), espone inevitabilmente ogni soggetto a rivelare parte di se al mondo esterno con il rischio potenziale, meno trascurabile di quanto si possa pensare, che altri soggetti possano accedere, anche remotamente, ai contenuti strettamente personali archiviati nei dispositivi stessi.

Va ricordato inoltre che non sempre è possibile, a meno di non ricorrere a metodi sofisticati o fortemente "distruttivi", eliminare completamente queste informazioni anche dal dispositivo stesso. Le cose si complicano maggiormente se le informazioni sono riposte nella rete Internet con i *servizi cloud* o perché veicolate nelle comunicazioni cellulari.

E' bene ricordare inoltre che Internet è uno spazio virtuale dotato di memoria il più delle volte permanente.

---

[1] http://www.kaspersky.com/it/about/news/virus/2015/Indagine_Kaspersky_Lab_n_utente_su_quattro_non_comprende_i_rischi_delle_minacce_informatiche_mobile

[2] Linguaggio usato per descrivere altri dati.

[3] Trattasi di uno spazio Internet messo a disposizione, gratis o a pagamento, all'interno del quale l'utente può conservare i propri dati. Non ha una collocazione fisica definita.

Il fatto che i dispositivi elettronici costituiscano una sorta di agenda elettronica è confermato anche da frequenti casi di cronaca nei quali le informazioni in essi contenuti hanno costituito utili fonti di prova nelle indagini giudiziarie.

Questo tipo di analisi svolte sui dispositivi elettronici o sistemi informatici, con tecniche alle volte che sono poco note ai non addetti ai lavori, possono presentare talvolta complicanze anche piuttosto importanti sia sotto l'aspetto tecnico che giuridico e devono essere ben gestite dai tecnici e comprese anche dai giuristi.

Le criticità naturalmente possono essere diverse anche in relazione al tipo di dispositivo elettronico oggetto di analisi. Questo fa sì che la memoria di massa di un *personal computer* (il classico *hard disk*) comporti in genere meno oneri, in termini di complessità, della memoria principale di un dispositivo *mobile*.

Se pure solo nei prossimi capitoli si fornirà una più approfondita disamina della questione, si può comunque anticipare che queste analisi rientrano nel vasto mondo della *digital forensics*. Al suo interno infatti troviamo la *mobile forensics*, sottocategoria della stessa, che si caratterizza e distingue sia da un punto di vista tecnico che giuridico per quel che riguarda l'acquisizione delle prove.

Il presente lavoro avrà come *focus* principale proprio la *mobile forensics* in ambito penale e riguarderà i dispositivi elettronici mobili come gli *smartphone* da considerarsi, in ultima analisi, dei computer con l'integrazione di un modulo radio trasmittente/ricevente.

Si tratta di dispositivi che rappresentano spesso oggetti molto personali contenenti dati anche di altri soggetti e che quindi attivano esigenze di tutela dei diritti legati alla tutela della riservatezza e che ciononostante talvolta le indagini possono invadere con prepotenza. Il più delle volte questi dispositivi sono protetti da *password* testuali o biometriche e quanto di più svariato ci sia. Barriere che però anche in contrapposizione ai diritti di cui sopra devono essere violate se si vuole accedere ai dati. Quello delle protezioni è un mondo altamente dinamico (si pensi per es. alla crittografia) e spesso comunque fonte di complicazione alle indagini.

Nel processo di acquisizione della prova informatica, associata ad un *personal computer* o *smartphone*, inoltre ci si può imbattere in casistiche particolari ch in quanto tali possono apparire, ma solo in superficie, banali.

Per fare un esempio, si ipotizzi a riguardo che la polizia giudiziaria trovi acceso il dispositivo da analizzare. Il fatto di spegnere o lasciare acceso un *computer* o *smartphone,* dai quali si vogliono ricavare elementi probatori utili all'indagine pur presentandosi, di primo

acchito, un'operazione apparentemente priva di rilevanza può presentare invece delle insidie notevoli. Va segnalato che nel caso dello *smartphone,* di norma, le accortezze da utilizzare dovranno essere ancora maggiori in quanto è un sistema che, come poi si vedrà, pone tutta una serie di problematiche anche complesse qualora si voglia cristallizzare una situazione in un certo voluto istante temporale.

L'esempio appena esposto pone in rilievo già da subito le problematiche connesse alle indagini informatiche, argomento che sarà analizzato, con tutti i limiti del caso, con il presente lavoro.

Partendo dai principi generali della prova e dagli istituti ad essa connessi, si vedrà poi come l'eventuale incaricato delle indagini dovrà valutare la cosa e come dovrà comportarsi in termini giuridico operativi. Si vedrà se esistano delle *best practices* per acquisire diligentemente una prova e utilizzarla in modo efficacie in sede di giudizio.

L'argomento del "comportamento" non è affatto banale anche in situazioni di apparenti stati che possono presentarsi al momento dell'acquisizione della prova digitale come per esempio quello, sopra evidenziato, di spegnere o meno un dispositivo elettronico trovato acceso.

Non si tralascerà di far cenno nel prosieguo dei principali istituti volti alla ricerca della prova e delle novità introdotte dalla convezione di Budapest recepita con legge 48/2008.

CAPITOLO I.- CENNI PRELIMINARI SULLE VIGENTI DISPOSIZIONI IN TEMA DI «DIGITAL FORENSICS»

.-1 Introduzione

Appare utile dar cenno ai principali istituti coinvolti nell'ambito del processo penale che riguardano l'aspetto istruttorio, e più precisamente i mezzi di ricerca della prova ed i mezzi di prova. In merito ovviamente occorre tenere conto delle prescrizioni contenute nella Costituzione ed in particolare dell'articolo 111, comma 4[4], con cui si introduce il principio del contraddittorio nella formazione della prova. Esso prevede che la prova si formi di regola con il contributo dialettico delle parti davanti al giudice, sicché il contraddittorio assume un duplice valore: per un verso come metodo per accertare la verità e per l'altro come condizione di regolarità del processo.

Bisogna aggiungere una importante precisazione sulla funzione della prova nel giudizio. Si può sostenere che il giudice, nel risolvere la *quaestio facti*, si comporta come uno storico, perché accerta un fatto che è avvenuto nel passato con l'ausilio delle parti, come si diceva sopra[5]. Il mezzo con cui si ricostruisce il fatto sono appunto le prove, che non coincidono con il fatto da provare, ma atti o cose diverse da esso, dalla cui percezione il giudice argomenta che un fatto è avvenuto o meno. Le prove sono strumenti della ricostruzione dei fatti all'interno del processo.

Il libro terzo del Codice di Procedura Penale definito come il "diritto delle prove" stabilisce che al giudice è riservato il potere di decidere, mentre alle parti è attribuito il potere di ricercare le prove, di chiederne l'ammissione, di contribuire alla formazione delle stesse.

Per inciso il libro terzo si compone di questa struttura:

- Libro III: Prove Titolo I: Disposizioni generali (artt. 187-193)
- Titolo II: Mezzi di prova (art. 194-243)
- Titolo III: Mezzi di ricerca della prova (artt. 244-271)

[4]Art. 111, comma IV, Costituzione: «*Il processo penale è regolato dal principio del contraddittorio nella formazione della prova. La colpevolezza dell'imputato non può essere provata sulla base di dichiarazioni rese da chi, per libera scelta, si è sempre volontariamente sottratto all'interrogatorio da parte dell'imputato o del suo difensore*».

[5] Si prende in considerazione la tesi della maggior parte della dottrina.

La prova è un procedimento che segue un percorso logico e razionale attraverso il quale dalla conoscenza di un fatto noto si vuole dedurre l'esistenza del fatto storico che si vuol provare. L'art. 187 del c.p.p. (oggetto della prova) chiarisce cosa è oggetto di prova[6]. In base a questo articolo possono essere oggetto di prova i fatti che si riferiscono all'imputazione, alla punibilità e alla determinazione della pena o della misura di sicurezza.

Il giudice inoltre può sulla base dell'art.189 del c.p.p. assumere prove non disciplinate dalla legge[7] se esse risultano idonee ad assicurare l'accertamento dei fatti e non pregiudicano la libertà morale della persona. In particolare ne subordina l'ammissione ad un contraddittorio tra le parti che vanno ascoltate circa le modalità di acquisizione della prova.

Il codice di procedura penale distingue fra mezzi di prova e mezzi di ricerca della prova: nella prima categoria rientrano la testimonianza, il documento, l'esame delle parte, il confronto, la perizia; nella seconda rientrano le perquisizioni, le ispezioni, i sequestri e le intercettazioni.

Gli atti che appartengono alla prima categoria solitamente sono compiuti in dibattimento o in incidente probatorio, mentre i mezzi di ricerca della prova si collocano nella fase dell'indagine e sono disposti sia dal giudice che dal Pubblico Ministero. Questi atti servono al Pubblico Ministero ai fini delle sue determinazioni o meno dell'esercizio delle azioni penali.

I mezzi di prova si caratterizzano per l'attitudine ad offrire al giudice risultanze probatorie direttamente utilizzabili in sede di decisione mentre i mezzi di ricerca della prova non sono in quanto tali fonte di convincimento ma rendono possibile accertare cose materiali, tracce.

Con riferimento ai mezzi di ricerca della prova converrà far cenno alla convenzione di Budapest, per poi comunque riprenderla nel prosieguo in modo più articolato, la quale ha fortemente interessato questi istituti, modificandoli allo scopo di intervenire con efficacia proprio nel campo delle analisi forensi digitali.

Fino al 2008 nonostante esistessero già delle norme che disciplinassero le ispezioni e le perquisizioni informatiche, sotto l'aspetto operativo esisteva una lacuna normativa relativamente all'intervento sui sistemi informatici con modalità tecniche adeguate e, spesso,

---

[6] art. 187 CPP: 1. *Sono oggetto di prova i fatti che si riferiscono all'imputazione, alla punibilità e alla determinazione della pena o della misura di sicurezza. 2. Sono altresì oggetto di prova i fatti dai quali dipende l'applicazione di norme processuali. 3. Se vi è costituzione di parte civile, sono inoltre oggetto di prova i fatti inerenti alla responsabilità civile derivante dal reato.*

[7] Art. 189 CPP: *Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti [187] e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova.*

si confondevano le prove digitali con i supporti materiali in cui queste erano racchiuse[8]. La prova informatica infatti è connotata da due caratteristiche specifiche che sono l' immaterialità e la fragilità. La legge di ratifica alla convenzione di Budapest (La legge 18 marzo 2008 n. 4 recante: «Legge 18 marzo 2008 n. 48: «Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno". in Gazzetta Ufficiale n. 80 del 4 aprile 2008 - Supplemento Ordinario n. 79) » ha colmato gran parte di queste lacune. Sino ad allora pochi addetti ai lavori, per lo più stranieri, operavano secondo standard procedurali, tutto sommato riconosciuti dalle procure come pratiche standard di indagini. Di ciò si ha contezza già con l'art. 247[9] comma 1 bis del c.p.p. dove si distingue tra prove digitali e oggetti contenitori.

Si cominciano con questa nuova fase a introdurre elementi sulle misure e proceduralità da adottarsi ai sistemi informatici o telematici atti a conservare e non alterare i dati originali.

Dunque la legge n.48/2008 si incardina su dei principi fondamentali quali la necessità di misure tecniche che garantiscano la conservazione dei dati originali e l'adozione di procedure che non alterino gli stessi.

La convenzione si caratterizza comunque non solo per le misure da adottarsi nell'acquisizione dei dati informatici ma estende la sua azione riformatrice anche ai dati sul traffico delle reti consentendo alle autorità di ordinare la conservazione di tali dati anche se detenuti presso terzi (provider).

La legge 48/200 è intervenuta sul codice penale e sul codice di procedura penale, ha in questo innovato le disposizioni relative ai mezzi di ricerca della prova (ispezioni, perquisizioni e sequestro) disposti dal pubblico ministero o nei caso di urgenza dalla polizia giudiziaria.

Pertanto il legislatore ha regolamentato le prassi investigative informatiche che, come sottolineato in precedenza, in parte venivano già adottate in ambito giudiziario pur non essendo ancora standardizzate.

---

[8] Cosi M. DANIELE, La prova digitale nel processo penale, Rivista di Diritto Processuale, 2011 «Una traccia di questa più risalente e fuorviante concezione emerge in modo chiaro dal previgente art. 491 bis c.p. che indentificava il "documento supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli» p. 284

[9] Articolo 247 CPP- Casi e forme delle perquisizioni: 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.*

La legge ha ricondotto talune modalità di acquisizione dei dati informatici durante le indagini preliminari all'interno dei mezzi tipici di ricerca della prova e considerate talvolta come atipici.

Dopo tali doverose premesse sull'evoluzione degli istituti regolatori delle indagini nel campo digitale, si affronteranno di seguito gli argomenti ritenuti essenziali all'oggetto del presente lavoro con la cura di scansionarli secondo un ordine che rispecchi una logica rispondente alle caratteristiche proprie delle analisi digitali.

Motivo per cui *in primis* si vuole affrontare la questione in termini generali cominciando dalla prova scientifica ed al suo ingresso nel processo. A ciò seguirà una esposizione degli istituti coinvolti relativamente alla fase delle indagini, e quindi i mezzi di ricerca della prova e degli istituti concernenti la fase del giudizio per passare ai mezzi di prova e finire poi con delle considerazioni di sintesi e conclusive.

.-2 Il problema della prova scientifica

Si affronta ora, in generale, il concetto della prova scientifica e delle problematiche a questa connessa.

Nella determinazione della prova digitale, considerata l'informatica un sapere scientifico, la conoscenza tecnico-scientifica assume un ruolo importante. In generale dove vengono richieste competenze scientifiche il giudice può affidarsi a soggetti esperti che hanno specifiche competenze. Per esempio, analizzare nel dettaglio un *file system*[10] di un qualsivoglia sistema operativo[11] di un computer per accertare se si sono verificate eventuali alterazioni fraudolenti, richiede strumenti di analisi e competenze personali specifiche, analogamente a quanto avviene e nel caso di una perizia ingegneristica per determinare la

[10] Una esatta definizione di *file* è difficile. Ma in generale indica un gruppo di informazioni omogenee. La lingua inglese lo intende con due significati: archivio e sequenza ordinata di elementi uguali e questo fatto ha un'origine "storica".Il *file system* è quella parte del sistema operativo di un *computer*, o dispositivo analogo come ad esempio un *mobile device*, atto a occuparsi dell'organizzazione dei *file*. A.TANEBAUM, *Architettura del computer. Un approccio strutturato*, MILANO, 2000, p. 429 definisce il *file* un'astrazione logica che ci permette di memorizzare le informazioni su disco e leggere in seguito e nella sua forma più semplice consiste in una sequenza di byte. La caratteristica più importante di questo meccanismo di astrazione è la denominazione del *file*. Quando un processo crea un *file* gli da un nome. Il *file* permette di implementare i meccanismi di Input/Output virtuali. Per il sistema operativo il processo di apertura di un *file* consente al sistema operativo di individuarlo sul disco e portare nella memoria le informazioni necessarie ad accedervi.

[11] Difficile definire in modo esatto un sistema operativo. Il compito di un sistema operativo può essere visto come quello di fornire un'allocazione metodica e controllata del processore, della memoria e dei dispositivi di input/output condivisi con vari programmi. Un sorta di direttore di orchestra.

causa del cedimento di un ponte. Ciò è previsto dall'art. 220 del c.p.p.[12]. che stabilisce che il giudice nomina il perito quando occorre svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze tecniche, scientifiche o artistiche. Persone cioè che hanno conoscenze specialistiche in quella determinata disciplina.

L'esperto potrà, solo sulla base delle leggi scientifiche, a lui note, individuare le cause dei fatti di cui si vuol dar conto[13] e non certo assumere verità costruite su termini probabilistici senza indicare una metodologia scientifica comprovata.

Rimane inteso però che l'applicazione delle leggi scientifiche non è sempre uno schema procedurale esente da imperfezioni, anche perché l'interpretazione delle stesse potrebbe essere imperfetta.

Il carattere delle leggi scientifiche è comunque quello della loro ripetibilità attraverso procedure note, sperimentate e consolidate. Le leggi scientifiche sono inoltre sempre oggetto di verifica degli esperti e questo rappresenta anche una forma di garanzia di un costante controllo della loro validità.

La prova nel processo penale è ammessa, si ricorda, perchè chiesta dal giudice sulla base dell'art. 190 del c.p.p.[14]. Deve essere pertinente, non vietata dalla legge, non superflua e rilevante.

Il giudice valuta la prova sulla scorta dell'art. 192 del c.p.p.[15] dando conto delle motivazioni dei risultati acquisiti e dei criteri adottati e quindi anche, per logica deduzione, sulla base delle leggi scientifiche utilizzate.

---

[12] Articolo 220 CPP Oggetto della perizia: *1. La perizia è ammessa quando occorre svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze tecniche, scientifiche o artistiche. 2. Salvo quanto previsto ai fini dell'esecuzione della pena o della misura di sicurezza, non sono ammesse perizie per stabilire l'abitualità (cp 102) o la professionalità (cp 105) nel reato, la tendenza a delinquere (cp 108), il carattere e la personalità dell'imputato e in genere le qualità psichiche indipendenti da cause patologiche.*

[13] Interessa qui Corte di Cassazione, sezione III penale, sentenza 16 gennaio 2014 (dep. 5 marzo 2014), n. 10491 rileva che i periti non agiscono con rigore scientifico ma solo su basi pseudo probabilistiche " *Ma, come si duole il ricorrente, la Corte territoriale non fornisce una risposta puntuale nemmeno ai vari punti, richiamati in premessa ed oggetto di specifiche allegazioni sia in appello che dinanzi a questa Corte di legittimità, in cui i periti avevano dichiarato di poter esprimersi solo in termini probabilistici e non di certezza circa ciò che era accaduto*"

[14] Articolo 190 CPP - Diritto alla prova: *1. Le prove sono ammesse a richiesta di parte. Il giudice provvede senza ritardo con ordinanza (125) escludendo le prove vietate (191) dalla legge e quelle che manifestamente sono superflue o irrilevanti (att. 38).2. La legge stabilisce i casi in cui le prove sono ammesse di ufficio (70, 195 ss., 210, 224, 422, 441, 468, 507, 511,603,633) 3. I provvedimenti sull'ammissione della prova possono essere revocati sentite le parti in contraddittorio.*

[15] Articolo 192 CPP - Valutazione della prova: *1. Il giudice valuta la prova dando conto nella motivazione dei risultati acquisiti e dei criteri adottati. 2. L'esistenza di un fatto non può essere desunta da indizi a meno che questi siano gravi, precisi e concordanti. 3. Le dichiarazioni rese dal coimputato del medesimo reato o da persona imputata in un procedimento connesso a norma dell'articolo 12 sono valutate unitamente agli altri elementi di prova che ne confermano l'attendibilità. 4. La disposizione del comma 3 si applica anche alle dichiarazioni rese da persona imputata di un reato collegato a quello per cui si procede, nel caso previsto dall'articolo 371 comma 2 lettera b).*

Si definisce scientifica quella prova che, partendo da un fatto dimostrato, utilizza una legge scientifica per accertare l'esistenza di un ulteriore fatto da provare. Poiché il rapporto tra il fatto noto e quello da provare è espresso da una regola, la prova scientifica rientra nella più vasta categoria della prova critica o indizio.

Non è facile dare una esatta definizione di scienza[16] ma con una certa generalità, si può definire scienza quel tipo di conoscenza che ha per oggetto i fatti della natura e che, è ordinata secondo un insieme di regole generali che sono denominate leggi scientifiche che sono in relazione tra loro secondo coerenza logica e sistematica.

In questo contesto scientifico l'evoluzione del concetto di prova nel tempo è legato anche all'evoluzione della scienza.

A differenza del passato dove la scienza appariva come infallibile e dove veniva intesa come verità assoluta, ora le leggi scientifiche[17] non perdono mai la loro natura di ipotesi di cui è sempre possibile dimostrare la falsità.

Non esiste legge scientifica che sia universale ed eterna perché nuove osservazioni e nuovi studi possono sempre metterle in discussione. Si pensi ad esempio alla fisica Newtoniana (meccanica classica) e poi quella relativistica di Einstein che ha rivoluzionato la meccanica classica.

Nella prova scientifica si usano strumenti di conoscenza attinti dalla scienza e dalla tecnica.

Si è detto che il giudice nel processo opera come uno storico, poiché deve ricostruire un fatto del passato, e questo può avvenire con documenti, testimonianze, e altro ancora, o con strumenti scientifici propri dello scienziato.

Il processo si "evolve" aprendosi alle nuove frontiere scientifiche al fine di trarne nuovi strumenti di indagine e di valutazione. La scienza per converso può attivare nuovi strumenti tecnici e metodologie operative sempre più perfezionate al processo.

Resto inteso inoltre che la prova scientifica deve fornire un'informazione valida e necessaria altrimenti non è utile al processo. La prova è inammissibile se fondata su criteri

---

[16] Dalle Garzantine Enciclopedia tematica Scienze 2007 Milano, p.1323, giova anche la definizione di scienza "termine con cui si indica un sistema di conoscenze organizzate checonsente di giungere a conclusioni verificabili"

[17] Da http://www.onorarimilano.it/documentazione/D_476.doc - Marco Maria ALMA, «*L'ingresso della prova scientifica nel processo penale (quesiti, tipi di accertamenti, rapporti con periti e consulenti ecc.) con particolare riguardo all'evoluzione nel tempo ed alla fallibilità della scienza in rapporto alla decisione da adottarsi «al di là di ogni ragionevole dubbio*» - Consiglio Superiore della Magistratura commissione per la formazione della Magistratura Onoraria Distretto della Corte d'Appello di Milano, Milano, 9 febbraio 2010.. Le leggi scientifiche utilizzabili dal giudice sono quelle connotate da elevato grado di conferma empirica per il superamento di tentativi di falsificazione secondo la concezione di Karl Raimund Popper.

scientifici inattendibili. Al pari dei teoremi matematici dove basta una sola argomentazione contraria per dimostrarne l'invalidità, così accade per la prova scientifica[18]. Come tutti i teoremi matematici anche le prove sono sottoposte a tentativi di falsificazione per confermare, qualora abbiano esito negativo, la validità. Deve essere inoltro noto l'errore che comportano e quindi il grado di validità[19].

Introdotto il concetto di scienza e prova scientifica, ora si vuole ora proseguire con una più articolata esposizione, con i naturali limiti del caso, partendo dalla dottrina.

Della prova scientifica[20], in ambito processuale, conviene prendere spunto per l'appunto dagli enunciati della dottrina che, per prima, occupandosi dell'argomento, ha stabilito con autorevolezza un fondamentale punto di partenza, ovvero che parlando di scientificità della prova il termine prova ha comunque diversi possibili significati.

Con il termine prova *in primis* si da significato in particolare al "risultato di prova" che è costituito dalle valutazioni alle quali il giudice perviene in relazione all'esistenza del fatto da provare *factum probandum*. L'autorevole dottrina indica come meno meritorio, riferendosi alla scientificità della locuzione prova il suo impiego nel senso di "mezzo di prova" in quanto il dato probatorio *factum probans* non ha di per se carattere di scientificità.

Analogo il discorso riferito alla prova come procedimento probatorio, anche se qui l'assunzione della prova comporta l'utilizzo di mezzi tecnici anche complessi in quanto trattasi di attività processuali preordinate.

---

[18] Così J. RESTON, Galileo, Casale Monferrato (AL), 2001 pag. 51: " … in queste sue annotazioni si era imposto uno standard elevato di accuratezza logica e sperimentale " In questo trattato il metodo da noi seguito sarà sempre tale da far si che tutto ciò che viene detto dipenda da quanto è stato affermato in precedenze, nei limiti del possibile, mai verrà dato per certo ciò che invece dovrà essere sperimentato...". Si tratta di una biografia di Galileo Galilei. Il brano si riferisce al pensiero dello scienziato.

[19] Interessa a riguardo il caso Vierika (Tribunale penale monocratico di Bologna I sezione n. 1823/2005 depositata in cancelleria il 22.12.205). Il giudice afferma, in termini generali, che anche quando il metodo utilizzato dalla Polizia Giudiziaria non dovesse ritenersi conforme alle migliore pratica scientifica, in difetto di prova di una alterazione concreta, conduce a risultati che sono, secondo quanto previsto dall'art.192 CPP., liberamente valutabili dal giudice: " *Occorre innanzitutto precisare che non è compito di questo Tribunale determinare un protocollo relativo alle procedure informatiche forensi, ma semmai verificare se il metodo utilizzato dalla p.g. nel caso in esame abbia concretamente alterato alcuni dei dati ricercati. In altre parole, non è permesso al Tribunale escludere a priori i risultati di una tecnica informatica utilizzata a fini forensi solo perché alcune fonti ritengono ve ne siano di più scientificamente corrette, in assenza della allegazione di fatti che suggeriscano che si possa essere astrattamente verificata nel caso concreto una qualsiasi forma di alterazione dei dati e senza che venga indicata la fase delle procedure durante la quale si ritiene essere avvenuta la possibile alterazione".* Anche uando anche il metodo utilizzato sia conforme alla migliore pratica scientifica ma però conduca a risultati che sono, per il principio di cui all'art. 192 CPP., liberamente valutabili dal giudice alla luce del contesto probatorio complessivo il giudice può considerare attendibili gli esiti delle operazioni tecniche Le regole seguite dagli operatori erano IACIS International Association of Colloid and Interface Scientists - http://www.iacis.com/

[20] Così da Oreste Dominioni, *Prova scientifica (diritto processuale penale)*, in Enciclopedia del Diritto, VOLUME II, Milano, 2008 p. 976 – 998.

Si conviene pertanto di riservare alla locuzione “scientificità della prova” alla formazione del convincimento del giudice ciò che comporta l'impiego di conoscenze che vanno oltre il suo sapere ovvero oltre il “patrimonio di conoscenza dell'uomo medio”.

Traccia di queste affermazioni si ritrovano nelle tipologie di incarichi assegnabili all'esperto (perito , consulente tecnico) e dei quali si darà cenno nel prosieguo.

Si ricavano, qui di seguito sommariamente elencati, diversi momenti di congiunzione nella ricerca della scienza nell'azione probatoria:

- Acquisire dati
- Svolgere indagini
- Fare valutazioni.

Fatte salve queste premesse sulla scientificità della prova e sul significato che il termine di prova assume va osservato e chiarito che comunque la scientificità non determina una categoria normativa autonoma e aggiuntiva rispetto ai “mezzi probatori”.

Necessita ancora precisare che gli istituti della perizia e della consulenza tecnica sono mezzi di prova che hanno in se una componente scientifica ma non determinano un categoria autonoma della prova scientifica.

Giova, nel sottolineare che i mezzi probatori si distinguono in “mezzi di prova” e “mezzi di ricerca della prova”, giova evidenziare che i mezzi di ricerca della prova non hanno una forma unitaria come i mezzi di prova che va pertanto ricostruita per ogni loro singola figura.

Nella struttura dei mezzi di prova si rinviene una componente ulteriore identificabile come “strumento di prova” costituita da apparati conoscitivi quali per esempio i principi di scienza applicata, tecnica, tecnologica e apparecchiature tali da uscire dalla classica sfera della “conoscenza comune” e per le quali si richiede l'intervento e il saper di un esperto.

Anche qui interessa chiarire che quali strumenti impiegare e i contenuti tecno-scientifici da utilizzare non rientrano nella competenza della legge ma in quello della scienza.

Questi strumenti scientifici, mutevoli come il sapere e l'esperienza, sono sempre indefiniti e reversibili e continuamente aggiornabili. Non esiste, in sostanza, una definitiva cristallizzazione della legge e dell'esperienza scientifica in quanto mutevole nel tempo e sempre oggetto di revisione. Non è poi compito della legge intervenire sulle modalità della loro validazione.

Nella pratica processuale vi sono strumenti scientifici e tecnici che hanno una ben consolidata, diremmo anzi "collaudata", sperimentazione e che quindi garantiscono, fino a prova contraria, un accertata validità. Non sempre però e così.

Ogni nuova scoperta scientifica, se pur determinata e riconosciuta, può abbisognare di un ulteriore vaglio della comunità scientifica e questa rappresenta una criticità nella considerazione del fatto che manca ancora una sorta di certificazione comunitaria conclusiva.

Naturalmente anche il campo giudiziario deve "testare" il nuovo strumento scientifico in modo tale da farlo entrare nell'esperienza giudiziaria non potendo costituire il solo mondo scientifico il validatore assoluto.

Va soppesato inoltre anche il fatto che uno strumento scientifico-tecnico può assumere carattere controverso, essendo possibili giudizi di segno opposto o anche perché dopo una prima accettazione il concetto scientifico viene messo o rimesso in discussione. E ancora si significa che lo strumento scientifico deve superare il giudizio della sfera giuridica.

Per la prova scientifica "comune" valgono le regole probatorie ordinarie mentre quelle che impiegano strumenti scientifici "nuovi" dove cioè vengono impiegati strumenti tecno-scientifici nuovi valgono regole "speciali".

Quindi se per la prima ci si riconduce alle regole dettate dall'art. 190[21] del c.p.p., per le seconde viene in rilievo l'art. 189[22] del c.p.p.

L'art. 189 del c.p.p. quando contempla le "prove non disciplinate dalla legge" («*Quando e` richiesta una prova non disciplinata dalla legge*») sembra riferirsi alle prove atipiche non disciplinate dalla legge quelle previste dal "catalogo legale".

E' atipica la prova che non rientra nel "catalogo legale" ed è consentita purché non violi precetti tassativi (*contra legem*) si da consentire l'ingresso nel processo penale di prove non previste dalla legge.

Spesso è discussa la necessità di consentire l'atipicità probatoria circa la sua applicabilità alla prova scientifica.

---

[21] Articolo 190 CPP - Diritto alla prova: *1. Le prove sono ammesse a richiesta di parte. Il giudice provvede senza ritardo con ordinanza (125) escludendo le prove vietate (191) dalla legge e quelle che manifestamente sono superflue o irrilevanti (att. 38). 2. La legge stabilisce i casi in cui le prove sono ammesse di ufficio (70, 195 ss., 210, 224, 422, 441, 468, 507, 511, 603, 633). 3. I provvedimenti sull'ammissione della prova possono essere revocati sentite le parti in contraddittorio.*

[22] Articolo 189 CPP - Prove non disciplinate dalla legge: *1. Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova.*

Pur tuttavia si riconosce senza equivoci[23] all'art. 189 del c.p.p. l'ammissione della prova scientifica. Sorreggono tale tesi, oltre a quanto argomentato, l'idoneità ad assicurare la ricostruzione del fatto e l'assenza di pregiudizio per la libertà morale della persona

L'idoneità probatoria nell'ammissione di nuove prove scientifiche ex art. 189 del c.p.p. deve possedere alcuni requisiti quali[24]:

- «la validità teorica del principio e metodologia scientifica» (strumentazione compresa)

- « l'adeguatezza dello strumento scientifico»

- « la controllabilità del corretto uso pratico dello strumento scientifico-tecnico»

- « la qualificazione dell'esperto»

- « la comprensibilità dello strumento probatorio scientifico – tecnico» che in sostanza deve essere comprensibile al sapere comune.

Quando sia ritenuta ammissibile una nuova prova scientifica dal giudice e, una volta chiarito da questo che la sua assunzione avvenga con modalità atipiche, egli deve stabilire che deve essere esercitata nel contraddittorio delle parti.

Va compiuta con l'obiettivo di rendere affidabile la ricostruzione delle parti atte alla prova del diritto.

Per prima cosa il giudice dovrà affrontare il problema della validità e affidabilità della prova scientifica. Alla validità si può pervenire attraverso le conoscenze della tecnica stessa mentre per l'idoneità si richiede che la stessa prova scientifica sia processualmente valida. Il giudice non deve poi affidarsi ciecamente al perito ma deve accertarsi che la prova scientifica sia razionalmente sostenibile e deve inoltre verificare la completezza della prova ovvero che si siano valutate tutte le situazioni possibili.

Un secondo stadio della valutazione si svolgerà in giudizio nella cosidetta "dialettica interna"seguendo[25]:

- verifica incrociata dei giudizi di attendibilità degli esiti della prova

- misurazione grado di efficacia dei risultati della prova

- grado complessivo di efficacia dei risultati probatori

- formulazione del *factum probans* e suo confronto con il *thema probandun*

- enunciazione dei fatti principali in termini di esistenza o inesistenza in relazione alle conclusioni dei precedenti giudizi.

[23] Così l'autorevole dottrina nell'Enciclopedia del Diritto.
[24] O. DOMINIONI, Prova scientifica (diritto processuale penale), cit., p. 985.
[25] *Ivi*, p. 991.

Argomento di un certo interesse in merito alla prova scientifica lo si ritrova in una sentenza degli Stati Uniti che costituisce un fondamento in questo tema. Pur se emessa in un giudizio civile e all'interno del *common law* è valido argomento da cui trarre spunto. L'oggetto della causa era costituito dagli effetti teratogeni di un farmaco antinausea in relazione al quale erano stati promossi diversi giudizi tutti però con sentenze sfavorevoli. La Corte aveva dato torto ai ricorrenti. La sentenza Daubert comunque indica i sottoelencati criteri di affidabilità delle teorie scientifiche[26] :

- Verificabilità: una teoria è verificabile se può essere controllata mediante esperimenti

- Falsificabilità: se la teoria scientifica sottoposta a tentativi di falsificazione non fallisce allora è credibile

- Conoscenza del tasso di errore: al giudice deve essere reso noto il tasso di errore

Quindi nessuna legge scientifica è immutabile e irreversibile.

Il giudice inoltre dovrà sempre comprendere pienamente il problema con uno studio preliminare dello stesso e non potrà propendere, per esempio, per la tesi peritale del Consulente Tecnico d'Ufficio. Inoltre non dovrà delegare agli esperti le questioni giuridiche del caso e sarà il più possibile *peritus peritorum*.

.-3 Mezzi di ricerca della prova e mezzi di prova nel vigente Codice di Procedura Penale

È noto che i mezzi di ricerca della prova non sono in quanto tali fonte di convincimento ma rendono possibile accertare cose materiali, tracce o dichiarazioni dotate di attitudine probatoria[27]; i mezzi di prova si caratterizzano per l'attitudine ad offrire al giudice risultanze probatorie direttamente utilizzabili in sede di decisione.

Gli atti che appartengono alla categoria dei mezzi di prova di regola sono compiuti in dibattimento, mentre i mezzi di ricerca della prova si collocano nella fase dell'indagine e sono

[26] Marco Maria ALMA - Cnsiglio superiore della magistratura commissione per la formazione della magistratura onoraria distretto della corte d'appello di milano relazione dal titolo «*L'ingresso della prova scientifica nel processo penale (quesiti, tipi di accertamenti, rapporti con periti e consulenti ecc.) con particolare riguardo all'evoluzione nel tempo ed alla fallibilità della scienza in rapporto alla decisione da adottarsi «al di là di ogni ragionevole dubbio*», Milano, 9 febbraio 2010.

[27] P. TONINI, *Manuale di procedura penale*, 11 ed., Milano, 2010 p. 366.

disposti sia dal giudice che dal Pubblico Ministero. Questi atti servono al Pubblico Ministero ai fini delle sue determinazioni o meno dell'esercizio delle azioni penali.

Caso speciale è rappresentato dall'incidente probatorio ex art. 392 c.p.p. (TITOLO VII - Incidente probatorio) che è un dispositivo processuale che permette l'anticipazione della formazione della prova nella fase delle indagini preliminari. Questo meccanismo deroga al principio per cui la prova si formi in dibattimento nel contraddittorio delle parti dinanzi a un giudice in quanto, attraverso l'intervento incidentale del giudice, è possibile l'acquisizione della prova, sempre nelle forme del contraddittorio, già durante le indagini preliminari.

Alcuni di questi possono essere assunti solo in presenza dei «casi tassativi di non rinviabilità al dibattimento» previsti dall'art. 392 c.p.p.:

- la testimonianza e il confronto
- l'esperimento giudiziale e la perizia aventi ad oggetto persone, cose o luoghi il cui stato è soggetto a modificazione non evitabile
- la perizia di lunga durata, che se disposta durante il dibattimento determinerebbe una sospensione superiore a sessanta giorni;
- la ricognizione in particolari casi d'urgenza

Vi sono mezzi di prova che possono essere assunti su mera richiesta di parte:

- l'esame dell'indagato che debba deporre su fatti concernenti la responsabilità altrui;
- l'esame dell'imputato (o indagato) connesso o collegato;
- su richiesta del difensore, la testimonianza o l'esame delle persone che si sono avvalse della facoltà di non rispondere all'intervista difensiva;
- la testimonianza di un minore di sedici anni in procedimenti per delitti di violenza sessuale, tratta di persone o assimilati.

In questa sede, per esigenze di linearità nell'esposizione delle questioni, si trattano prima i mezzi di ricerca della prova e poi i mezzi di prova.

.....3.1.- Mezzi di ricerca della prova

Alla luce di questa breve ma necessaria premessa si vuole ora dar cenno agli istituti dei mezzi di ricerca della prova.

.....3.1.1.- Le ispezioni

L'ispezione (art. 244[28] c.p.p) consiste nell'osservare e descrivere persone, luoghi e cose allo scopo di accertare le tracce e gli altri effetti materiali del reato. E' uno strumento che risente della materialità strutturalmente legata al suo oggetto che riguarda per l'appunto le tracce egli altri effetti materiali del reato[29].

E' un mezzo di ricerca della prova che ha prevalentemente una finalità descrittiva di persone, luoghi e cose ed è disposta, di regola, dall'autorità giudiziaria quando occorre *«accertare le tracce e gli altri effetti materiali del reato*» (art. 244, comma 1) . In ogni caso, l'Autorità Giudiziaria, può disporre rilievi ed ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione (art. 244, comma 2 , mod. dalla legge n. 48 del 2008).

L'ispezione può svolgersi anche con l'impiego di poteri coercitivi. Poiché il potere coercitivo incide su libertà protette dalla Costituzione, il codice prevede determinate formalità per le ispezioni delle persone e dei luoghi; in ogni caso, l'ispezione è disposta con decreto motivato.

Il secondo comma dell'art. 244 del c.p.p. pone un problema importante quando si riferisce all' utilizzo metodologie atte a impedire alterazioni del dato originale. Il dato digitale è infatti facilmente alterabile sopratutto nella fase di acquisizione dal sistema informatico. Saranno essenziali strumenti tecnici e software costruiti allo scopo e l'utilizzo di procedure consolidate dall'esperienza tecnica e scientifica.

.....3.1.2.- Le perquisizioni

L'istituto della perquisizione può prodursi in sede di indagini preliminari su iniziativa del Pubblico Ministero e delegandola alla Polizia Giudiziaria. Nell'articolo 247[30] del c.p.p. si

[28] Articolo 244 CPP - Casi e forme delle ispezioni: *1. L'ispezione delle persone, dei luoghi e delle cose (103) è disposta con decreto motivato (125) 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, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.*

[29] M. DURANTE, U. PAGALLO, Manuale di informatica giuridica e diritto delle tecnologie, Torino, 2012 p.255.

[30] Articolo 247 CPP- *Casi e forme delle perquisizioni: 1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando*

ritrovano casi e forme delle perquisizioni. Essa può essere personale o locale. Si ha il caso di personale quando si ritiene un soggetto occulti sulla persona il corpo del reato. La perquisizione locale è disposta quando le cose si trovino in un determinato luogo.

L'articolo 247 del c.p.p. ha inoltre legami, in tema di accertamenti urgenti della Polizia Giudiziaria, con l'art. 354 del c.p.p. anch'esso modificato.

La legge n. 48/2008 ha modificato l'articolo 247 dopo il comma 1 in quanto ha inserito il comma 1-bis novellando che 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. Ha altresì modificato l'articolo 248[31] comma 2 primo periodo sostituendo la parte «atti, documenti e corrispondenza presso banche»» con le seguenti: «presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici».

E' di interesse notare che il legislatore ha dato maggiore forza e invasività ai poteri degli investigatori prevedendo anche la possibilità di superare le misure di protezione poste a tutela del sistema informatico o telematico che sia.

Il legislatore si cura anche della necessità di adottare misure tecniche tali da non alterare i dati. Appare quindi interessante notare che il comportamento da adottarsi dagli inquirenti con un dispositivo acceso o spento perchè le azioni da adottarsi, alla luce della necessità della non alterazioni dei dati, sarà diversa.

Altra considerazione andrà fatta tenendo conto che l'attività in questione è prodromica a quella di sequestro. In definitiva però sconsiglierà il sequestro di un data center[32] di un

---

vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo (att. 75) ovvero che in esso possa eseguirsi l'arresto dell'imputato (293, 380 ss.) o dell'evaso (cp 385), è disposta perquisizione locale (103, 250; coord. 225). 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. (1) 2. La perquisizione è disposta con decreto motivato (125). 3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria (57) delegati con lo stesso decreto (103).

[31] Articolo 248 CPP - Richiesta di consegna: 1. *Se attraverso la perquisizione si ricerca una cosa determinata, l'autorità giudiziaria può invitare a consegnarla. Se la cosa è presentata, non si procede alla perquisizione, salvo che si ritenga utile procedervi per la completezza delle indagini. 2. Per rintracciare le cose da sottoporre a sequestro (253) o per accertare altre circostanze utili ai fini delle indagini, l'autorità giudiziaria o gli ufficiali di polizia giudiziaria da questa delegati possono esaminare presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici. (1) In caso di rifiuto, l'autorità giudiziaria procede a perquisizione (255).*

[32] Centro elaborazione dati composto da numerosi elaboratori.

istituto finanziario. Le esigenze di continuità lavorativa imporranno la copia dei soli dati ritenuti utili.

.....3.1.3.- Il sequestro

Il codice prevede tre distinte forme di sequestro: il sequestro «probatorio« (art. 253), il sequestro «preventivo« (art. 321[33]) e il sequestro «conservativo« (art. 316[34]).

Il primo è collocato tra i mezzi di ricerca della prova; gli altri due tra le misure cautelari.

Comune ai tre tipi di sequestro è la caratteristica di creare un vincolo di indisponibilità su una cosa mobile od immobile, attraverso uno spossessamento coattivo. Differenti sono le finalità delle tre misure che, di conseguenza, hanno una distinta regolamentazione.

---

[33] Articolo 321 CPP- *Oggetto del sequestro preventivo: 1. Quando vi è pericolo che la libera disponibilità di una cosa pertinente al reato possa aggravare o protrarre le conseguenze di esso ovvero agevolare la commissione di altri reati, a richiesta del pubblico ministero il giudice competente a pronunciarsi nel merito ne dispone il sequestro con decreto motivato (262). Prima dell'esercizio dell'azione penale (405) provvede il giudice per le indagini preliminari (328). 2. Il giudice può altresì disporre il sequestro delle cose di cui è consentita la confisca (cp 240). 2-bis. Nel corso del procedimento penale relativo a delitti previsti dal capo I del titolo II del libro secondo del codice penale il giudice dispone il sequestro dei beni di cui è consentita la confisca. (1). 3. Il sequestro è immediatamente revocato a richiesta del pubblico ministero o dell'interessato quando risultano mancanti, anche per fatti sopravvenuti, le condizioni di applicabilità previste dal comma 1. Nel corso delle indagini preliminari provvede il pubblico ministero con decreto motivato, che è notificato a coloro che hanno diritto di proporre impugnazione. Se vi è richiesta di revoca dell'interessato, il pubblico ministero, quando ritiene che essa vada anche in parte respinta, la trasmette al giudice, cui presenta richieste specifiche nonché gli elementi sui quali fonda le sue valutazioni. La richiesta è trasmessa non oltre il giorno successivo a quello del deposito nella segreteria (2). 3-bis. Nel corso delle indagini preliminari, quando non è possibile, per la situazione di urgenza, attendere il provvedimento del giudice, il sequestro è disposto con decreto motivato dal pubblico ministero. Negli stessi casi, prima dell'intervento del pubblico ministero, al sequestro procedono ufficiali di polizia giudiziaria, i quali, nelle quarantotto ore successive, trasmettono il verbale al pubblico ministero del luogo in cui il sequestro è stato eseguito. Questi, se non dispone la restituzione delle cose sequestrate, richiede al giudice la convalida e l'emissione del decreto previsto dal comma 1 entro quarantotto ore dal sequestro, se disposto dallo stesso pubblico ministero, o dalla ricezione del verbale, se il sequestro è stato eseguito di iniziativa dalla polizia giudiziaria (3). 3-ter. Il sequestro perde efficacia se non sono osservati i termini previsti dal comma 3bis ovvero se il giudice non emette l'ordinanza di convalida entro dieci giorni dalla ricezione della richiesta. Copia dell'ordinanza è immediatamente notificata alla persona alla quale le cose sono state sequestrate (3).*

[34] Articolo 316 CPP- Presupposti ed effetti del provvedimento: 1. *Se vi è fondata ragione di ritenere che manchino o si disperdano le garanzie per il pagamento della pena pecuniaria (660), delle spese di procedimento e di ogni altra somma dovuta all'erario dello Stato, il pubblico ministero, in ogni stato e grado del processo di merito, chiede il sequestro conservativo dei beni mobili o immobili dell'imputato o delle somme o cose a lui dovute, nei limiti in cui la legge ne consente il pignoramento. 2. Se vi è fondata ragione di ritenere che manchino o si disperdano le garanzie delle obbligazioni civili (cp 185) derivanti dal reato, la parte civile può chiedere il sequestro conservativo dei beni dell'imputato o del responsabile civile, secondo quanto previsto dal comma 1. 3. Il sequestro disposto a richiesta del pubblico ministero giova anche alla parte civile. 4. Per effetto del sequestro i crediti indicati nei commi 1 e 2 si considerano privilegiati (cc 2745), rispetto a ogni altro credito non privilegiato di data anteriore e ai crediti sorti posteriormente, salvi, in ogni caso, i privilegi stabiliti a garanzia del pagamento dei tributi.*

Il sequestro probatorio previsto dall'art. 253[35] del c.p.p. è un mezzo di ricerca della prova e consiste nell'assicurare una cosa mobile o immobile al procedimento per finalità probatorie, mediante lo spossessamento coattivo della cosa e la creazione di un vincolo di indisponibilità sulla medesima.

Deve essere un bene materiale come è necessario anche un requisito «giuridico», e cioè che si tratti del corpo del reato o di una cosa pertinente al reato e in particolare fondamentale che la cosa sia «necessaria» per l'accertamento dei fatti.

Il sequestro è mantenuto fino a quando sussistono le esigenze probatorie (art. 262, comma l)[36] e ha come limite massimo la sentenza irrevocabile oltre il quale la cosa deve essere restituita, salvo confisca.

Anche qui la legge n.48/2008 ha agito con modifiche agli artt. 254, 259, e 260 del c.p.p.

All'art. 254 del c.p.p il legislatore è intervenuto anche nel sequestro per corrispondenza associato a forme telematiche "fornitori di servizi postali, telegrafici, telematici e di telecomunicazione" ampliando il suo raggio di azione e guardando quindi anche agli Internet Service Provider.

Dopo l'art 254 del c.p.p. viene inserito 254-*bis*[37]. Mentre l'art 254 (Sequestro di corrispondenza) prevede che "*presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica*", qualora l'autorità giudiziaria abbia motivo di ritenere possono avere relazione con il reato, l'art. 254-bis (Sequestro di dati informatici presso fornitori di servizi informatici,

---

[35] Articolo 253 CPP - Oggetto e formalità del sequestro: *1. L'autorità giudiziaria dispone con decreto motivato (125) il sequestro del corpo del reato e delle cose pertinenti al reato necessarie per l'accertamento dei fatti. 2. Sono corpo del reato le cose sulle quali o mediante le quali il reato è stato commesso nonché le cose che ne costituiscono il prodotto, il profitto o il prezzo. 3. Al sequestro procede personalmente l'autorità giudiziaria (57) ovvero un ufficiale di polizia giudiziaria delegato con lo stesso decreto (103). 4. Copia del decreto di sequestro è consegnata all'interessato, se presente (att. 81)*.

[36] Articolo 262 CPP - *Durata del sequestro e restituzione delle cose sequestrate: 1. Quando non è necessario mantenere il sequestro a fini di prova, le cose sequestrate sono restituite a chi ne abbia diritto, anche prima della sentenza. Se occorre, l'autorità giudiziaria prescrive di presentare a ogni richiesta le cose restituite e a tal fine può imporre cauzione.*

[37] Articolo 254-bis CPP (Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni). - 1.*L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni,* dei *dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali*

telematici e di telecomunicazioni) prevede che l'autorità giudiziaria, quando dispone il sequestro presso i fornitori di servizi informatici e telematici, può stabilire che la loro acquisizione avvenga mediante copia si essi su adeguato supporto naturalmente con procedura atta a conservarne l'originalità. A ciò che è posto sotto sequestro probatorio bisogna garantire la genuinità e la non alterabilità. Questo però è rivolto non al computer o alla memoria di massa bensì al documento informatico. Da ciò deriva che la clonazione ovvero il clone della memoria di massa è vero oggetto del sequestro.

Il legislatore si adegua all'evoluzione tecnologica con l'art. 260[38] c.p.p. (Apposizione dei sigilli alle cose sequestrate. Cose deperibili. Distruzione di cose sequestrate) , con il quale è prevista la possibilità da parte delle autorità di assicurare, garantire e certificare, le cose sequestrate anche attraverso l'apposizione di sigilli di carattere elettronico o informatico così da creare il vincolo imposto ai fini di giustizia. Il chiaro intento è quello di certificare la copia e l'originale per mezzo di procedure informatiche che nella sostanza si riconducono alle funzioni di hash[39].

Spesso il tema del sequestro è stato tra dottrina e giurisprudenza tema piuttosto dibattuto[40]. Più che di sequestro fisico legato ad un disco rigido è prevalso il concetto che ci si debba invece riferire ad un sequestro logico attraverso la copia dei dati ottenuto con la tecnica del *bit stream image*.

Il secondo comma estende la presunzione di deperibilità e alterazione prevedendo la possibilità di effettuare copia su supporti adeguati mediante una procedura che ne assicuri la conformità all'originale.

---

[38] Articolo 260 CPP comma 1 - Apposizione dei sigilli alle cose sequestrate. Cose deperibili. Distruzione di cose sequestrate: 1. *Le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario e con le sottoscrizioni dell'autorità giudiziaria e dell'ausiliario che la assiste ovvero, in relazione alla natura delle cose, con altro mezzo, anche di carattere elettronico o informatico, idoneo a indicare il vincolo imposto ai fini di giustizia*.

[39] Una funzione di hash accetta come input una stringa di bit di lunghezza arbitraria e produce un risultato di dimensione fissa (digest). Il risultato è un "condensato" chiamato digest, ha una dimensione fissa e ha tipicamente una lunghezza compresa tra i 128 e 1024 bit. Deve avere la caratteristica di essere una funzione non reversibile, e deve avere una resistenza alle collisioni ovvero dati due stringhe in ingresso diverse non si deve avere lo steso digest. Se pure rappresenta un fatto altamente improbabile nessuna funzione di hash è immune alle collisioni. Così da Schneier Bruce Niel Ferguson – Bruce Schneier – Tadayoshi KohnoIl, Manuale della crittografia – p. 71-74_

[40] «*Netta è la posizione della Cassazione che nella sentenza n. 735/2007 afferma come l'acquisizione indiscriminata di informazioni, rectius dati, contenuti all'interno della memoria di un computer non può e non deve risolversi in una distorsione delle attività d'indagine volte alla ricerca della notitia criminis. In un caso analogo ha sostenuto ad ampie lettere come "l'atto acquisitivo, non individuando in maniera chiara e specifica il legame intercorrente fra il reato per cui si procedeva e l'azione di sequestro dell'intera memoria informatica, si è risolto in una acquisizione indiscriminata (...)" generando l'illegittimità del sequestro stesso»* http://www.altalex.com/documents/news/2012/05/03/i-nuovi-mezzi-di-ricerca-della-prova-fra-informatica-forense-e-l-48-2008

.....3.2.- Mezzi di prova

Si vogliono ora prendere in considerazione in termini generali, i principali mezzi di prova. Su alcuni ci si soffermerà in modo maggiore essendo di sicuro interesse per le indagini forensi. Gli istituti come la testimonianza, l'esame delle parti, confronti, ricognizioni ed esperimenti giudiziali, su cui ci soffermerà solo brevemente, non rappresentano particolarità nelle indagini digitali.

.....3.2.1.- L'esperimento giudiziale

L'esperimento giudiziale è ammesso quando occorre accertare se un fatto sia o possa essere avvenuto in un determinato modo (art. 218 del c.p.p.)[41]. L'esperimento consiste nella riproduzione, nei limiti del possibile, della situazione in cui il fatto si afferma verificato o si ritiene essere avvenuto e nella ripetizione delle modalità di svolgimento del fatto stesso. Considerato che il fatto storico di reato è irripetibile lo scopo dell'esperimento è quello di accettare la corrispondenza della ricostruzione del fatto stesso riproducendone le modalità di svolgimento.

La validità dell'esperimento è tanto più attendibile quanto più esiste la possibilità di riprodurre esattamente, in un momento temporalmente successivo al fatto originale, tutte le condizioni nelle quali si afferma essere avvenuto per l'appunto il fatto da ricostruire.

L'impossibilità di riprodurre fedelmente siffatte condizioni potrebbe costituire il limite naturale dell'esperimento.

.....3.2.2.- La perizia

La perizia è un mezzo di prova finalizzato ad integrare le conoscenze del giudice con quelle di un esperto. Essa deve essere disposta dal giudice quando occorre compiere una valutazione per la quale sono necessarie specifiche competenze tecniche, scientifiche o artistiche e che non mirano a definire l'abitualità o la professionalità nel reato o il carattere e la personalità dell'imputato. La perizia adempie alle tre seguenti funzioni che richiedono, per essere esercitate, speciali conoscenze: 1) svolgere indagini per acquisire dati probatori; 2)

[41] Articolo 218 CPP - *Presupposti dell'esperimento giudiziale: 1. L'esperimento giudiziale è ammesso quando occorre accertare se un fatto sia o possa essere avvenuto in un determinato modo. 2. L'esperimento consiste nella riproduzione, per quanto è possibile, della situazione in cui il fatto si afferma o si ritiene essere avvenuto e nella ripetizione delle modalità di svolgimento del fatto stesso.*

acquisire gli stessi dati selezionandoli e interpretandoli; 3) effettuare valutazioni sui dati già acquisiti (art. 220, comma 1). L'incarico è conferito a persona che sia qualificata, dal punto di vista tecnico e professionale, scelta preferibilmente tra gli iscritti in appositi albi, che divisi in categorie, sono tenuti presso i tribunali.

Tra i compiti del perito vi può essere quello di percepire quei dettagli del fatto noto, che soltanto un tecnico può identificare o quello di applicare ad un fatto noto una legge scientifica, in modo da fornire una valutazione al giudice.

Il testimone espone un fatto, mentre il perito dà una valutazione su di un fatto al fine di indicare la legge scientifica ad esso applicabile. In realtà, a volte la perizia è anche una prova rappresentativa di ciò che il perito ha fatto o percepito nell'adempimento dell'incarico.

La perizia non è l'unico mezzo di prova che permette di raggiungere le finalità indicate nell'art. 220 del c.p.p. La consulenza tecnica consiste nel conferimento ad un esperto del mandato di esporre il proprio parere, ovviamente nell'interesse della parte che lo ha nominato (art. 233 del c.p.p.).

Anche se il codice non ricomprende espressamente i consulenti tecnici tra i mezzi di prova, si ritiene comunque che tali esperti possano fornire elementi utili per la decisione rendendo superflua la nomina di un perito.

Interesse si ravvisa nella sentenza della Corte di Cassazione Penale (Cass.Pen. 11 agosto 2004 n.34379) con la quale si afferma di non poter gravare sul giudice l'onere di "fornire autonoma dimostrazione dell'esattezza scientifica" delle tesi sostenute dal perito d'ufficio e dal consulente di parte[42].

Questo istituto viene utilizzato nella prassi delle indagini digitali.

[42] ANDREA, GIRARDINI, GABRIELE FAGGIOLI, Digital Forensics, Milano Apogeo 2013, p. 25 " la Corte di Cassazione ha più volte stabilito che "*in tema di controllo sulla motivazione, il giudice che ritenga di aderire alle conclusioni del perito d'ufficio, in difformità da quelle del consulente di parte,non può essere gravato dell'obbligo di fornire autonoma* dimostrazione *dell'esattezza scientifica delle prime e dell'erroneità, per converso,delle altre, dovendosi al contrario considerare sufficiente che egli dimostri di avere comunque valutato le conclusioni del perito d'ufficio, senza ignorare le argomentazioni del consulente; ne consegue che può ravvisarsi vizio di motivazione solo se queste ultime siano tali da dimostrare in modo assolutamente lampante e inconfutabile la fallacità delle conclusioni peritali*"

.....3.2.3.- La prova documentale

Il requisito è indicato nell'art. 234, comma 1[43] dove si contempla che perché vi sia un documento è sufficiente che si tratti di uno scritto oppure di un oggetto comunque idoneo a rappresentare un fatto, una persona o una cosa.

Non è rilevante l'operazione mediante la quale la rappresentazione è incorporata e che pertanto può essere la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo[44].

Sempre con riferimento all'art. 234 del c.p.p. è possibile tracciarne una più articolata definizione e cioè quella rappresentazione di un fatto che è incorporata su di una base materiale attraverso il metodo analogico e il metodo digitale.

Con il metodo digitale, che in questa sede ha maggior interesse, la rappresentazione è incorporata su di una base materiale mediante grandezze fisiche discrete ossia variabili con discontinuità: si tratta di stati logici numeri, zero e uno. Il dato che contiene l'informazione è denominato informatico ed è composto dalla sequenza di bit . L'incorporamento digitale ha la fondamentale caratteristica che è «immateriale» nel senso che la rappresentazione esiste indifferentemente dalla scelta del tipo di supporto fisico sul quale il dato informatico è incorporato; infatti, il documento informatico[45] , definito dall'art. 1 comma 1 lett. p d.lgs 7 marzo 2005 come "rappresentazione" informatica di atti, fatti, o dati giuridicamente rilevanti, può essere trasferito facilmente da un supporto all'altro, anche se per la sua esistenza fisica ne richiede comunque uno. Ad esempio, il supporto fisico può essere l'*hard disk*, o una *pen drive*, o un altro strumento idoneo a "contenere" il dato originale.

Per i giuristi rilevano due difficoltà: come abbiamo accennato, il dato informatico è facilmente modificabile e inoltre, in alcuni casi un successivo accesso al file tramite il dispositivo (es. personal computer) provoca la modifica del contenuto dello stesso.

Per tali motivi, può essere arduo conservare un documento informatico inalterato, in modo da assicurare che la prova sia autentica e genuina. Di qui la necessità di particolari

---

[43] Articolo 234 CPP- Prova documentale: *1. È consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo. 2. Quando l'originale di un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita copia. 3. È vietata l'acquisizione di documenti (191) che contengono informazioni sulle voci correnti nel pubblico intorno ai fatti di cui si tratta nel processo o sulla moralità in generale delle parti, dei testimoni (196), dei consulenti tecnici e dei periti*.

[44] PAOLO TONINI, *Manuale di procedura penale*, cit., p. 371.

[45] La definizione legislativa di documento informatico è rinvenibile nell'art. 1 D.Lgs. 7 marzo 2005, n. 82 (codice dell'amministrazione digitale), in cui si precisa che per documento informatico si intende «la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti » (lett.p) e per documento analogico « la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti » (lett. p-bis).

cautele, come ad esempio la creazione di una copia-clone dell'*hard disk* conforme all'originale, che viene resa non modificabile mediante appositi procedimenti.

.-4 Considerazioni di sintesi sulla prova digitale nella disciplina del processo penale

La legge 48/2008 ha novellato i mezzi di ricerca del codice di procedura penale della prova con particolare riferimento a ispezioni, perquisizioni e sequestri.

Le modifiche apportate agli istituti testè menzionati riguardano l'acquisizione dei dati informatici affinché ne venga garantita l'integrità attraverso misure tecniche dirette ad assicurare la conservazione dei dati originali ed impedire l'alterazione proprio a seguito dell'intervento di chi indaga, salvaguardando in tal modo il diritto di difesa.

Come si è accennato la prova informatica ha la caratteristica della immaterialità e volatilità, motivo per cui bisogna agire secondo dettami tecnici particolari.

La legge 48/2008 ha di fatto ricondotto nei mezzi tipici di ricerca l'ispezione, la perquisizione, l'ispezione e il sequestro di un sistema informatico.

Interessa notare che con la legge n. 48/2008 relativamente ad un supporto magnetico (*hard disk*) di un computer posto sotto sequestro a essere conservata è la sua copia clone.

La legge inoltre non è intervenuta sul sequestro in generale ma se si vuole sul sequestro per corrispondenza e presso i fornitori di servizi informatici, telematici e di telecomunicazioni.

Ha senso ora precisare con maggior dettaglio riassumendo alcuni concetti, già considerati all'interno dei principali istituti, al fine di verificare come la norma ha recepito e novellato il codice di procedura penale in alcuni punti che ora si descriveranno[46]:

- art. 244 comma 2 del c.p.p.(ispezioni) con aggiunta " *anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione* "

- art. 247 comma 1-bis del c.p.p. (perquisizioni) " *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*."

[46] D'AIUTO G., LEVITA L., I reati informatici disciplina sostanziale e questioni processuali, Milano, 2012 pp.120-121.

- art. 254 bis del c.p.p. (Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni) "*L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali*"

- art. 256 del c.p.p. (Dovere di esibizione e segreti) "*nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto*"

- art. 259 del c.p.p. (Custodia delle cose sequestrate) "*Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria. Al custode può essere imposta una cauzione. Dell'avvenuta consegna, dell'avvertimento dato e della cauzione imposta è fatta menzione nel verbale. La cauzione è ricevuta, con separato verbale, nella cancelleria o nella segreteria"*.

- art. 352 comma 1-bis del c.p.p. (Perquisizioni) "*Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previste, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi*"

- art. 354 del c.p.p. (Attività a iniziativa della polizia giudiziaria) "*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*"

Queste modificazioni trovano la loro ratio comune nella preoccupazione di rendere compatibile l'attività di sequestro con la genuinità dei dati originali e di garantire la conformità delle copie agli originali.

Il legislatore ha dunque regolamentato le prassi investigative informatiche che in parte avvenivano già, come sottolineato in precedenza, in ambito giudiziario ma non ancora standardizzate.

Naturalmente su alcune questioni rimangono ancora delle incertezze e perciò che di seguito si riportano alcune considerazioni relative agli aspetti più delicati legati a questo tema.

.....4.1.- Problematiche legate alla copiature dei dati

Il sequestro di un documento informatico attraverso la *bitstream image* [47] o clonazione di un *hard disk* non può essere ricondotto nelle previsioni dell'art. 258 del c.p.p al pari dell'acquisizione di una copia di un documento cartaceo.

Per clonazione qui si intende la copia immagine dell'originale ovvero ottenuta con copiatura bit per bit[48] che deve contenere anche lo spazio non allocato[49].

Il nuovo art. 254-bis del c.p.p. fa sì che la clonazione di un *hard disk* dal punto di vista giuridico è un sequestro informatico.

Anche dal punto di vista pratico e operativo si pongono delicate questioni concernenti la riservatezza, ed in particolare la tutela della sfera privata delle persone che, pur non essendo destinatarie del provvedimento di sequestro, sono comunque interessate ai dati personali raccolti. Si pensi per esempio a tutti gli interlocutori di comunicazioni elettroniche, a soggetti a cui si riferiscono i documenti informatici contenuti nelle memorie analizzate, alle persone ritrattate nelle immagini contenute negli archivi informatici.

---

[47] Copia forense informatica

[48] Siamo alla copia dell'unità elementare logica

[49] Anche qui il problema si vedrà potrebbe aprirsi potenzialmente con i dischi allo stato solido SSD. I dischi SSD (Solid State Drive) sono delle unità a stato solido sono cioè memorie basate su semiconduttore (memorie flash). Torna molto utile anche nel prosieguo comprendere che un disco allo stato solido opera in maniera completamente diversa da un disco magnetico tradizionale. Su quest'ultimo i piatti sono magnetizzati con una serie di zero e uno e quando si cancella un *file* si svuota (dal punto di vista logico) una parte del disco, permettendo di utilizzarla in futuro per l'allocazione di altri *file*. La struttura dati di un SSD non è quella di un HDD (Hard Disk Drive), ovvero una pista continua che contiene i *file*, ma si ragiona seguendo le dimensioni fisiche delle celle di memoria. Ogni cella può contenere un numero finito di dati e la loro lettura può avvenire anche in contemporanea. Per questo motivo viene meno la necessità di avere dati solo sequenziali e, anzi, in alcuni casi le prestazioni massime si hanno leggendo in parallelo da più celle distinte. La scrittura su un SSD avviene infatti per blocchi. Un blocco, che ha dimensione normale di 256 Kbyte deve in ogni caso essere scritto per intero ogni volta. Questo significa, ad esempio, che modificare un singolo bit presente in questo blocco porta alla necessità, da parte del Ssd, di cancellare l'intero blocco e riscriverlo con il bit in questione modificato. La discrepanza tra il mondo operativo e quello elettrico è insita proprio qui: per il sistema operativo è stato scritto 1 solo bit, mentre per l'SSD il processo di scrittura è stato di 256 Kbyte. Il problema è che ciò non si ripercuote solo sulle prestazioni del sistema ma risiede nel fatto che questa cancellazione è un'operazione usurante, la cella di memoria si consuma a ogni scrittura effettuata.

Il problema della copia può essere piuttosto delicato perché come si vedrà poi anche nel prosieguo del capitolo essa potrebbe ancora non essere una perfetta clonazione dell'originale.

.....4.2.- La catena di custodia

A corollario della volatilità ed alterabilità del dato informatico[50] in una generalità più ampia, resta la necessità di definire, ai fini della sua utilizzabilità in ambito forense, un procedimento acquisitivo che preservi e garantisca la genuinità del dato, sotto il duplice profilo della autenticità e della integrità dello stesso.

La garanzia deve essere assicurata in ogni intervento di sopralluogo della polizia giudiziaria (vale per ogni altro operatore) e nel sequestro disposto dall'autorità giudiziaria. Questa garanzia ha attuazione attraverso la catena di custodia (chain of custody) e cioè tramite la corretta documentazione di ogni passo del procedimento attuato per l'acquisizione e analisi dei dati.

Ora, va sottolineato come, dal punto di vista del diritto processuale penale, l'integrità e l'autenticità della prova digitale siano elementi che assumono grande rilievo ai fini di una eventuale declaratoria di inutilizzabilità della prova raccolta ovvero - secondo un differente approccio, per la verità meno condivisibile - ai fini di una riduzione del suo valore probatorio in sede di apprezzamento giudiziale. Certamente, si potrà dire, le cautele per assicurare la preservazione della evidenza digitale criminosa non sono sconosciute al sistema processuale, essendo in parte già applicate ad esempio ai settori dell'analisi di campioni biologici. Tuttavia essendo di fronte ad una prova la cui natura è volatile, alterabile e falsificabile quale è il dato digitale, si richiede un bagaglio di standard procedurali capaci di garantire attendibilità all'accertamento penale. Per ottenere questo risultato occorre assicurare la cosiddetta continuità probatoria, ossia la possibilità di tenere traccia del procedimento di repertamento ed analisi in ogni suo punto mediante la produzione di report a vari livelli di dettaglio, grazie ai

[50] Può tornare utile dare una definizione di cosa si intenda per dato informatico anche quella riportata - all'art.2 definizioni - della nella DIRETTIVA 2013/40/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 12 agosto 2013 relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio - L 218/8 Gazzetta ufficiale dell'Unione europea 14.8.2013 che li definisce come una rappresentazione di fatti, informazioni o concetti in una forma che può essere trattata in un sistema di informazione, compreso un programma atto a far svolgere una funzione a un sistema di informazione. A sua volta per sistema di informazione viene inteso come un'apparecchiatura o gruppo di apparecchiature interconnesse o collegate, uno o più dei quali svolge un trattamento automatico di dati informatici secondo un programma, nonché i dati informatici immagazzinati da tale apparecchiatura o gruppo di apparecchiature, trattati, estratti o trasmessi dagli stessi ai fini della loro gestione, uso, protezione e manutenzione.

quali si potranno escludere «*alterazioni indebite delle tracce informatiche intervenute in epoca successiva alla creazione, trasmissione od allocazione in un supporto autorizzato*»[51]. Il mantenimento della prova in materia di investigazioni informatiche richiede allora una completa annotazione delle operazioni fisiche e informatiche compiute al momento dell'acquisizione del dato e nella successiva fase di conservazione, così da poterla addirittura ricostruire.

La catena di custodia, peraltro, è solo una delle componenti che contribuiscono a formare il "castello" di regole a protezione delle genuinità della prova elettronica, regole che entrano in gioco come si vedrà nella parte dedicata alla *digital forensics*, fin dall'arrivo degli investigatori sulla *scena criminis* digitale e che fanno del metodo di verifica forense un sistema trasparente e verificabile dalle altre parti processuali.

Si vuole qui fare riferimento al complesso interrogativo circa la ripetibilità o meno delle operazioni di *computer forensics* nelle successive fasi del procedimento. La questione appare di non poco rilievo, stabilito che un eventuale giudizio affermativo sulla loro capacità modificatrice dei dati informatici comporterebbe, come è noto, decisive conseguenze processuali quali la necessità di comunicativa alla difesa prima del compimento dell'atto e l'eventuale intervento di un consulente tecnico della persona indagata, senza contare i correlati problemi di inutilizzabilità degli accertamenti svolti in violazione di siffatte garanzie.

.....4.3.- La figura del consulente informatico

Il codice di procedura penale distingue fra perizia e consulenza ed entrambe consistono in indagini, accertamenti e valutazioni scientifiche e tecniche che possono essere disposte dal Pubblico Ministero, il Giudice, e le altre parti. Il perito è nominato dal giudice, il consulente è nominato dal pubblico ministero o dall'imputato.

Le analisi forensi dei sistemi informatici richiedono competenze specifiche, e cioè capacità tecnica e la necessità di motivare con capacità di formulazione di valutazioni critiche dei risultati di dette attività, e quindi sia la parte che l'autorità giudiziaria deve ricorrere a esperti del settore informatico.

[51] A.GIRARDINI, G. FAGGIOLI, *Digital Forensics*, cit., p.45.

Le analisi forensi possono essere condotte dalla Polizia, dei periti, da consulenti di parte C.P.T. o Consulenti Tecnici d'Ufficio C.T.U. i quali presenteranno (il mezzo di prova) una relazione conclusiva.

Secondo l'ordinamento italiano i tecnici se nominati da una delle parti rivestono il ruolo di C.T.P o se nominati dal giudice di C.T.U.

Le nomine avvengono ai sensi degli articoli 220 – 226[52] del c.p.p..

La perizia nel caso del C.T.U. ricorre inoltre quando vi sono indagini da svolgere che richiedono particolari competenze scientifiche o artistiche. L'incarico viene conferito in virtù del art. 226 del c.p.p.

Il perito dopo l'assegnazione dell'incarico sulla base degli artt. 228 - 230[53] del c.p.p. indica il giorno, l'ora e il luogo dell'inizio delle operazioni di verifica. Sulla base dell'art. 230 del c.p.p i periti di parte possono assistere al conferimento dell'incarico del perito e presentare richieste, osservazioni e riserve delle quali si è fatta menzione nel verbale.

---

[52] All'art. 220 del c.p.p. è utilizzata la formula «*La perizia è ammessa quando occorre svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze tecniche, scientifiche o artistiche*» non appena il giudice accerti la esistenza di un determinato tema di prova per il quale occorra svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze tecniche, scientifiche o artistiche.

Vi è una limitazione laddove viene stabilito espressamente, all'art. 220 comma 2, del c.p.p. «*salvo quanto previsto… ».*

Alla nomina del perito si applicano le regole poste nell'art. 221 c.p.p. come si rinviene al comma 1 «*Il giudice nomina il perito scegliendolo tra gli iscritti negli appositi albi o tra persone fornite di particolare competenza nella specifica disciplina. Quando la perizia è dichiarata nulla, il giudice cura, ove possibile, che il nuovo incarico sia affidato ad altro perito»*

Con gli artt. 222 e 223 del c.p.p si fa riferimento alla responsabilità disciplinare il perito che ha l'obbligo di presentarsi dinanzi al giudice nel giorno e nell'ora indicati nell'atto di citazione e di dichiarare se si trova in una condizione di incapacità, incompatibilità o di astensione.

Lo stesso perito deve adempiere al suo ufficio al solo scopo di far conoscere la verità e ha l'obbligo di rispettare il segreto nello svolgimento delle operazioni peritali, con la conseguenza che la violazione, da parte del perito, dei doveri previsti dalla legge da luogo a responsabilità disciplinare.

A norma dell'art. 224 del c.p.p. la perizia è richiesta d'Ufficio con l'indicazione del giorno, dell'ora e del luogo fissati per la comparizione del perito.

Il provvedimento è notificato alle parti che ai sensi dell'art. 225 del c.p.p. possono nominare i propri consulenti tecnici, i quali possono assistere alle operazioni peritali, proponendo al perito specifiche indagini e formulando osservazioni e riserve.

I consulenti delle parti (art. 226, comma 2, del c.p.p.) possono interloquire direttamente col perito e di poter ampliare anche i quesiti ovvero sulle questioni tecniche.

[53] Articolo 230 CPP. Attività dei consulenti tecnici: *1. I consulenti tecnici (coord. 223) possono assistere al conferimento dell'incarico al perito e presentare al giudice richieste, osservazioni e riserve, delle quali è fatta menzione nel verbale (136). 2. Essi possono partecipare alle operazioni peritali, proponendo al perito specifiche indagini e formulando osservazioni e riserve, delle quali deve darsi atto nella relazione (227). 3. Se sono nominati dopo l'esaurimento delle operazioni peritali, i consulenti tecnici possono esaminare le relazioni e richiedere al giudice di essere autorizzati a esaminare la persona, la cosa e il luogo oggetto della perizia. 4. La nomina dei consulenti tecnici e lo svolgimento della loro attività non può ritardare l'esecuzione della perizia e il compimento delle altre attività processuali.*

Articolo 231 CPP. Sostituzione del perito

Articolo 232 CPP. Liquidazione del compenso al perito

Articolo 233 CPP. Consulenza tecnica fuori dei casi di perizia

I periti di parte possono inoltre partecipare alle operazioni peritali del C.T.U. proponendo o formulando osservazioni e riserve che devono essere incluse nella relazione.

In merito all'esame orale del perito che ha svolto l'azione peritale l'art. 501[54] del c.p.p. prevede che per l'esame dei periti e dei consulenti tecnici siano osservate le disposizioni sull'esame dei testimoni. L'art. 511 del c.p.p. prevede al comma 3 che "*La lettura della relazione peritale è disposta solo dopo l'esame del perito*" ovvero che la relazione può diventare prova solo dopo l'esame orale del perito.L'ausiliario di polizia giudiziaria è nominato in virtù dell'art. 348[55] del c.p.p. per svolgere le indagini che devono accertare traccie o cose che potrebbero subire alterazioni ma non esprime valutazioni tecnico scientifiche.

.-5 Conclusione

La legge 48/2008 è intervenuta in tema di ispezione negli artt. 244 c.p.p. e di perquisizione all' art. 247 c.p.p. . Ancora meglio chiarisce il comma 2 dell'art. 244 c.p.p., in relazione a sistemi informatici e telematici, indicando di adottare le misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

Prima della convezione la dottrina e la giurisprudenza discutevano con riferimento al materiale informatico, con particolare riferimento alle attività di sequestro e di ispezione. La discussione verteva sulla necessità di acquisire tutto il supporto informatico o meno. La Cassazione per esempio (Cassazione V, 19 marzo 2002 Manganello) aveva ritenuto illegittimo il sequestro di un intero server ai fini probatori. Ma successivamente la stessa Corte si esprimeva in termini diversi ritenendo anche inutile il sequestro di materiale informatico

[54] Articolo 501 CPP - Esame dei periti e dei consulenti tecnici: *1. Per l'esame dei periti (220 ss.) e dei consulenti tecnici (225, 233) si osservano le disposizioni sull'esame dei testimoni, in quanto applicabili. 2. Il perito e il consulente tecnico hanno in ogni caso facoltà di consultare documenti, note scritte e pubblicazioni, che possono essere acquisite anche di ufficio.*

[55] Articolo 348 CPP - Assicurazione delle fonti di prova: *1. Anche successivamente alla comunicazione della notizia di reato, la polizia giudiziaria continua a svolgere le funzioni indicate nell'articolo 55 raccogliendo in specie ogni elemento utile alla ricostruzione del fatto e alla individuazione del colpevole (1). 2. Al fine indicato nel comma 1, procede, fra l'altro: a) alla ricerca delle cose e delle tracce pertinenti al reato nonché alla conservazione di esse e dello stato dei luoghi; b) alla ricerca delle persone in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti; c) al compimento degli atti indicati negli articoli seguenti. 3. Dopo l'intervento del pubblico ministero, la polizia giudiziaria compie gli atti ad essa specificamente delegati a norma dell'articolo 370, esegue le direttive del pubblico ministero ed inoltre svolge di propria iniziativa, informandone prontamente il pubblico ministero, tutte le altre attività di indagine per accertare i reati ovvero richieste da elementi successivamente emersi e assicura le nuove fonti di prova. (2) 4. La polizia giudiziaria, quando, di propria iniziativa o a seguito di delega del pubblico ministero, compie atti od operazioni che richiedono specifiche competenze tecniche, può avvalersi di persone idonee le quali non possono rifiutare la propria opera (att. 115).*

neutro rispetto alle indagini[56]. Conveniva infatti che sarebbe bastato, a tutelare la prova, il solo sequestro per esempio dell'*hard disk*.

Nei casi di un sequestro della polizia giudiziaria è importante di sequestrare quanto ritenuto utile ai fini dell'indagine, e rimettere in sostanza agli investigatori, che si presumono preparati allo scopo, l'oggetto del sequestro. Ecco quindi che il sequestro del materiale informatico deve pertanto essere valutato caso per caso.

Si è poi riscontrato un altro elemento utile, in termini di ispezioni e sequestro, che è quello di considerare il limite a disposizione come quando ci si trovi davanti ad una grande mole di dati, cosa che può avvenire pensando ad esempio ad un cluster di computer tipico di un *data center*.

Nell'esposizione dei principali istituti si è cercato di analizzare in particolare quelli o quelle parti che comportassero maggiori affinità tecnico giuridiche alle indagini forensi. Le analisi informatiche oltre a coniugare un aspetto fortemente tecnico debbono necessariamente legarsi e seguire quelle che sono le norme procedurali del processo penale. Si è visto che il legislatore ha dovuto seguire e aprirsi al mondo scientifico e tecnologico con adattamenti alle norme esistenti , in questo caso del codice di procedura penale, ed in particolare con la legge n.48/2008.

Relativamente alla prova scientifica si è cercato di fornire una adeguata trattazione in quanto ritenuta una componente fondamentale considerata per l'appunto la natura scientifica dell'informatica.

Il mondo digitale ha aperto nuove problematiche, ha definito nuove tipologie di documenti e prove come quelle informatiche. Probabilmente esistono ancora zone da esplorare come quella per esempio della copia digitale di cui si cercherà di affrontare nel prosieguo, aggiungendo qualche elemento di valutazione in più.

[56] Come le stampanti per esempio.

CAPITOLO II.- LA DIGITAL FORENSICS ED IL PROBLEMA DELL'ACCERTAMENTO IRRIPETIBILE

.-1 Introduzione

La *digital forensics*, estensione della preesistente *computer forensics* che costituiva e costituisce quel settore della *forensics* legato in modo principale al computer, potrebbe essere definita come quella disciplina scientifica, capace di individuare un fatto (prova digitale o *digital evidence*) inscindibilmente correlato ad un dispositivo elettronico o ad una rete informatica o telematica, e di riprodurlo in un processo attraverso la sua ripetibilità scientifica.

Il termine *digital* anteposto a *forensics* indica, rispetto a *computer forensics*, una gamma più estesa di dispositivi digitali tutti quelli cioè legati all'informazione digitale che trattano cioè informazioni di tipo discreto, elementari, costituita da stati logici – uno e zero – e che si contrappongono alla rappresentazione analogica rappresentata dal cosi detto continuo. Chiaro quindi che con il termine *digital* si ha l'aggancio ad un mondo molto più vasto della *computer forensics* ed è da sottolineare, dal punto di vista tecnico che gran parte dei dispositivi elettronici sono caratterizzati dal fatto di possedere una matrice comune condividendone spesso la stessa natura architetturale che è quella dei computer.

In verità la *digital forensics*, deve intendersi una locuzione a geometria variabile, che amplia i sui spazi di intervento anche a dei sotto settori come la *mobile forensics*, *network forensics*, e la nuova e più astratta (meglio virtuale) *cloud forensics*[57].

Anche se il presente lavoro avrà come focus principale la *mobile forensics* che comprende come "attori" principali e rappresentativi gli *smartphone* e *tablet*, va precisato, che questo è un insieme di dispositivi molto eterogeneo e in continua evoluzione.

[57] Conviene ora definire meglio il significato di cloud: Fonte http://www.ibm.com/cloud-computing/it/it/what-is-cloud-: Il cloud computing, o in forma abbreviata cloud, è la fornitura delle risorse di elaborazione on-demand, dalle applicazioni ai data center, su Internet così suddivise: - Le applicazioni SaaS (Software as a Service) o basate sul cloud vengono eseguite su *computer* remoti di proprietà e gestito da terzi, collegandosi dai *computer* degli utenti tramite Internet. - Le soluzioni PaaS (Platform as a Service) forniscono un ambiente basate sul cloud con tutte le risorse richieste per supportare l'intero ciclo di vita di sviluppo e fornitura delle applicazioni basate sul Web. - Il modello IaaS (Infrastructure as a Service) fornisce alle aziende le risorse di elaborazione, come server, rete, storage e spazio nei data centre su base «pay-per-use«.

Se possono inoltre definire in concreto alcuni campi d'azione della *digital forensics* in cui essa è di sicuro ausilio[58]: indagini interne ad un'azienda, supporto alla Polizia Giudiziaria ed ai PM (CTU), supporto ai privati indagati (CTP), valutazione danni, spionaggio, frode, pedopornografia, violazione policy aziendali, estorsioni, terrorismo.

.-2 Cenni generali sulla struttura costitutiva dei calcolatori elettronici

La *digital forensics* ha una componente, ma lo si è già anticipato, fortemente scientifica e tecnologica oltre che giuridica, motivo per il quale prima di affrontare il tema delle tecniche più comuni di analisi dei dispositivi elettronici, appare utile premettere qualche concetto di carattere tecnico sui dispositivi elettronici in genere.

Matrice comune di tutti questi dispositivi, in grande maggioranza elaboratori, è come ricordato una architettura sostanzialmente simile e alla cui base possiamo ritrovarvi la storica macchina di Von Neumann (1945) che costituisce, ancora oggi, il modello semplificato dei calcolatori moderni (unità centrale di elaborazione CPU[59], memoria centrale, interfacce di ingresso e uscita, bus).

Se si scompone virtualmente un calcolatore vi si ritrovano due macro componenti fondamentali come l'hardware e il software, anche se oggi la loro distinzione diventa sempre più complicata[60].

Gioverà al riguardo continuare a introdurre alcuni concetti tecnici correlati a queste componenti base allo scopo di ottenere vantaggio nella esplicazioni che seguiranno relativamente alle osservazioni di carattere informatico giuridico che verranno poi prese in considerazione.

Il calcolatore, in prima approssimazione come si è fatto cenno poc'anzi descrivendo la sua struttura, trova al suo interno come elemento fondamentale una CPU (Central Processing Unit) ovvero il cervello che esegue i programmi immagazzinati nella memoria centrale (principale) leggendo le relative istruzioni.

La memoria principale è quella zona dove vengono immagazzinati i programmi e i dati. L'unità base della memoria è un numero binario chiamato bit (in termini di capacità si

[58] N. BASSETTI*, Indagini digitali vademecum di uno Sherlock Holmes informatico*, 2011 p.7

[59] Essa si compone di parti distinte. L'unità di controllo che legge le istruzioni, l'unità di aritmetico-logica che esegue le operazioni. Contiene inoltre una memoria ad alta velocità che a sua volta contiene un certo numero di registri con diverse funzioni.

[60] "L'hardware non è null'altro che software pietrificato" così l'autore A.TANEBAUM, *Architettura del computer un approccio strutturato*, cit., p.8. Esempio concreto ne sono le macchine virtuali che emulano gran parte dell'*hardware*

usa il byte o suoi multipli) che può contenere uno 0 o un 1. E' questa di fatto una "aritmetica" che rende i calcolatori più efficienti.

La memoria principale non sempre riesce a essere capace tanto quanto si vorrebbe e per tale motivo la soluzione tradizionale per memorizzare una grande quantità di dati è la gerarchia di memoria. Ritroviamo così i tradizionali dischi magnetici *hard disk* elettromeccanici o quelli emergenti allo stato solido SSD, "penne" USB, CD/DVD-ROM e l'elenco potrebbe continuare.

Le memorie che si possono leggere e scrivere si chiamano RAM (Random Access Memory) e non costituiscono chiaramente tutto il panorama memorie. Si hanno quindi le ROM (Read Only Memories) che non si possono cambiare o cancellare, le PROM (Programmable ROM) le EEPROM la cosiddetta memoria flash (esempio la classica pendrive USB). L'elenco non è chiaramente esaustivo ma certamente esemplificativo.

Fin qui le parti hardware. Viene poi il sistema operativo che costituisce il necessario legante nonchè il coordinatore di tutte queste risorse. E' un componente essenziale da conoscere bene specie per attivare e gestire correttamente le tecniche di analisi informatiche.

Sarà su queste componenti hardware e software che insisterà l'analisi dei sistemi informatici e da queste si arguiranno e dedurranno le ipotesi probatorie dei vari casi.

.-3 Cenni sull'accertamento tecnico ripetibile e irripetibile

La legge n. 48/2008 ha previsto, in relazione ai mezzi di ricerca del documento informatico, alcuni tipi di garanzie fondamentali, che dovrebbero essere attuate in ognuno dei mezzi di ricerca della prova. Le garanzie sono così riassumibili:

- dovere di conservare inalterato il dato informatico originale nella sua genuinità.
- dovere di impedire l'alterazione successiva del dato originale.
- dovere di formare una copia che assicuri la conformità del dato informatico acquisito rispetto a quello originale.
- dovere di assicurare la non modificabilità della copia del documento informatico
- La garanzia della installazione di sigilli informatici sui documenti acquisiti.

Occorre segnalare che la legge n. 48 del 2008 non è stata sistematica, a causa della fretta con la quale è stata approvata[61]. Il Parlamento si è dimenticato ora di una, ora di un'altra

[61] http://leg15.camera.it/_dati/leg15/lavori/schedela/trovaschedacamera_wai.asp?PDL=2807. Da … testo copiato "in data 27febbraio 2008 è stata ratificata dal Senato la legge di ratifica alla Convenzione di Budapest del 23 novembre 2001 del Consiglio d'Europa; dopo un' appassionata ed eleborata analisi della normativa presso la Commissione riunite di Giustizia e Senato si è arrivati frettolosamente anche grazie ad un accordo fra

delle garanzie che, viceversa, sono necessarie tutte e in contemporanea nel caso di un mezzo di ricerca della prova informatica.

Le lacune non trovano una giustificazione logica se non nella sommarietà dell'approccio alla problematica del documento informatico. In casi come questo spetta alla dottrina e alla giurisprudenza ricomporre il sistema in via interpretativa. Con tutti i problemi che ciò comporta, visto che la materia attiene ad alcuni dei diritti fondamentali garantiti dalla Costituzione.

Con riferimento alla prova viene in rilievo l'accertamento tecnico informatico e la ripetibilità o irrepetibilità dello stesso.

Il tema è dibattuto perché non sempre è di facile soluzione. Vi sono situazioni di fatto astrattamente non modificabili, la cui intangibilità è quasi certa, mentre nel caso della sfera del digitale dove il dato da peritare, è come si è accennato immateriale e fragile soggetto cioè ad una facile alterazione[62]. Inoltre alcuni comportamenti di analisi richiedono alta professionalità e talvolta sono legate al momento dell'analisi.

Durante le indagini in generale è prassi eseguire accertamenti, rilievi descrittivi, fotografici o altre operazioni tecniche per le quali sono necessarie specifiche competenze e in questo caso si procede alla nomina di un consulente tecnico. L'accertamento tecnico è lo strumento di cui si dispone in tale eventualità, che sarà attuato dal consulente tecnico incaricato. Gli elementi che egli riuscirà a rilevare, se ammessi al processo, diventeranno mezzi di prova[63].

Nel nostro codice di procedura penale sono previste due diverse tipologie di accertamento tecnico, quello ripetibile e quello non ripetibile.

---

maggioranza ed opposizione , sel finire della legislatura all'approvazione ...". Utile anche atti precedenti che forse chiedevano al tempo al legislatore di prendere in considerazione le questioni digitali emergenti come la Raccomandazione n.R (95) 13 del Consiglio dei Ministri agli Stati membri relativa ai problemi di procedura penale legati alla tecnologia dell'informazione (adottata dal Consiglio dei Ministri l'11.9.1995, nel corso della 543^ riunione dei Delegati dei Ministri) da https://wcd.coe.int/ViewDoc.jspid=538519&Site=COE&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383 Rec(95)13E 11 September 1995 concerning problems of criminal procedural law connected with information technology COUNCIL OF EUROPE COMMITTEE OF MINISTERS RECOMMENDATION No. R (95) 13 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES CONCERNING PROBLEMS OF CRIMINAL PROCEDURAL LAW CONNECTED WITH INFORMATION TECHNOLOGY (Adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies). La rivista GNOSIS Rivista italiana di intelligence (Agenzia Informazioni e Sicurezza Interna) costituisce una autorevole fonte di traduzione http://gnosis.aisi.gov.it/s%5CRivista8.nsf/servnavig/14

[62] Il dump della memoria di un dispositivo acceso per esempio è un accertamento irripetibile. Una volta spento la situazione è, rispetto a prima, cambiata. Ma qualsiasi interazione con un dispositivo in linea teorica ne potrebbe pregiudicare lo stato originale.

[63] P. TONINI, *Manuale di procedura penale,* cit., p. 521.

Gli accertamenti tecnici ripetibili contemplano tutte quelle operazioni di indagine che possono essere ripetute nel tempo senza pregiudizio della loro attendibilità. Il riferimento normativo è previsto dall'art. 359 del c.p.p. che contempla la figura del consulente tecnico del pubblico ministero che procede ad eventuali "*accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze*". In tale eventualità il pubblico ministero nomina per l'appunto un consulente tecnico e fa svolgere l'accertamento coperto dal segreto investigativo, di cui comunque i difensori avranno facoltà di prendere visione ed estrarre copia ai sensi e per gli effetti dell'art. 433[64] del c.p.p. mediante l'avviso all'indagato della conclusione delle indagini preliminari ex. art. 415-bis[65] del c.p.p. Il verbale del predetto atto sarà inserito nel fascicolo del pubblico ministero.

Gli accertamenti tecnici irripetibili sono disciplinati all' art. 360 del c.p.p e seguenti.

Il Pubblico Ministero (senza ritardo) deve comunicare alle parti il giorno, ora e luogo fissato per il conferimento dell'incarico, dando loro notizia della possibilità di nominare consulenti tecnici, esattamente come avviene nel caso di una perizia. I difensori e i consulenti eventualmente incaricati hanno il diritto di partecipare agli accertamenti e di formulare osservazioni e riserve. In detti casi viene attribuita all'atto un'efficacia simile a quella della perizia, concordandone tra le parti il momento del suo effettivo svolgimento al fine di garantire un controllo ad opera dell'indagato.

---

[64] Articolo 433 CPP - Fascicolo del pubblico ministero 1. *Gli atti diversi da quelli previsti dall'articolo 431 sono trasmessi al pubblico ministero (51) con gli atti acquisiti all'udienza preliminare unitamente al verbale dell'udienza. 2. I difensori (96 ss.) hanno facoltà di prendere visione ed estrarre copia, nella segreteria del pubblico ministero, degli atti raccolti nel fascicolo formato a norma del comma 1. 3. Nel fascicolo del pubblico ministero (51) ed in quello del difensore è altresì inserita la documentazione dell'attività prevista dall'articolo 430 quando di essa le parti si sono servite per la formulazione di richieste al giudice del dibattimento (470) e quest'ultimo le ha accolte (reg. 19)*

[65] art. 415 bis CPP *1. Prima della scadenza del termine previsto dal comma 2 dell'articolo 405, anche se prorogato, il pubblico ministero, se non deve formulare richiesta di archiviazione ai sensi degli articoli 408 e 411, fa notificare alla persona sottoposta alle indagini e al difensore nonché, quando si procede per i reati di cui agli articoli 572 e 612 bis del codice penale, anche al difensore della persona offesa o, in mancanza di questo, alla persona offesa avviso della conclusione delle indagini preliminari (2). 2. L'avviso contiene la sommaria enunciazione del fatto per il quale si procede, delle norme di legge che si assumono violate, della data e del luogo del fatto, con l'avvertimento che la documentazione relativa alle indagini espletate è depositata presso la segreteria del pubblico ministero e che l'indagato e il suo difensore hanno facoltà di prenderne visione ed estrarne copia. 3. L'avviso contiene altresí l'avvertimento che l'indagato ha facoltà, entro il termine di venti giorni, di presentare memorie, produrre documenti, depositare documentazione relativa ad investigazioni del difensore, chiedere al pubblico ministero il compimento di atti di indagine, nonchè di presentarsi per rilasciare dichiarazioni ovvero chiedere di essere sottoposto ad interrogatorio. Se l'indagato chiede di essere sottoposto ad interrogatorio il pubblico ministero deve procedervi. 4. Quando il pubblico ministero, a seguito delle richieste dell'indagato, dispone nuove indagini, queste devono essere compiute entro trenta giorni dalla presentazione della richiesta (3). Il termine puó essere prorogato dal giudice per le indagini preliminari, su richiesta del pubblico ministero, per una sola volta e per non piú di sessanta giorni. 5. Le dichiarazioni rilasciate dall'indagato, l'interrogatorio del medesimo ed i nuovi atti di indagine del pubblico ministero, previsti dai commi 3 e 4, sono utilizzabili se compiuti entro il termine stabilito dal comma 4, ancorché sia decorso il termine stabilito dalla legge o prorogato dal giudice per l'esercizio dell'azione penale o per la richiesta di archiviazione*.

In sintesi ecco perché l'accertamento potrebbe non essere irripetibilità: «*1) "Non è ripetibile perché la modificazione dell'oggetto da esaminare è in atto" o è solo probabile […] 2) " Non ripetibile perché l'accertamento" modifica l'oggetto da esaminare […] 3) "Non ripetibile a causa del contesto in cui l'accertamento è compiuto" il che potrebbe far presumere tutto irripetibile […] 4) "Non ripetibile perché l'atto non è differibile" […] 5) "Non ripetibile perché l'atto di accertamento è compiuto a sorpresa" […] 6) "Non ripetibile perché l'accertamento" è ripetibile ma comporta la perdita in qualche modo dell'elemento di prova*»[66]

Vi è da aggiungere inoltre a riguardo le considerazioni già svolte circa la modificabilità della prova digitale. L'immaterialità della stessa e le peculiarità evidenziata in precedenza si sostanziano nella facilità con cui possono essere alterate da chiunque anche inavvertitamente e nel normale agire operativo. Questo fatto genera un alto rischio di cui dovrà essere tenuto conto anche nel modo di procedere in un accertamento tecnico ripetibile o non ripetibile. L'immaterialità è anche sinonimo di dispersione del dato essendo possibile la loro distribuzione in più luoghi. Infatti frequentemente le macchine server che li contengono hanno collocazioni fisiche anche molto distanti tra loro.

Pare interessante allo scopo, se non altro per una questione di concretezza, valutare per esempio se sia atto tecnico ripetibile o meno l'effettuazione di una copia clone dell'*hard disk* di un computer.

L'accertamento è ripetibile, in senso giuridico, come per esempio può avvenire avviene nel caso di un *hard disk* estratto a computer spento.

L'accertamento non è ripetibile se il suo compimento può avvenire soltanto una volta perché la sua ripetizione porta a risultati non genuini.

Converrà a riguardo fare qualche considerazione aggiuntiva, riportandosi all'esempio proposto nel capitolo introduttivo di questo elaborato, e poi ripreso arricchendolo anche di altre argomentazioni, e valutare il comportamento che l'operatore dovrebbe tenere durante un sequestro nel caso in cui trovasse il computer acceso, alla luce della ripetibilità o irrepetibilità dell'accertamento tecnico.

In prima battuta si potrà sostenere che qualora il computer sia spento o in stato di disallineamento, ci si trovi in una situazione "statica" e quindi dal punto di vista giuridico in

---

[66] P. TONINI, *Considerazioni su diritto di difesa e prova scientifica,* 2013, pp. 823-837 www.archiviopenale.it/apw/wp-content/.../06/il_punto_su_Tonini.pdf

una condizione di ripetibilità in quanto si potranno eseguire le azioni di copiatura delle memorie di massa secondo i dettami forensi richiesti.

Per converso, qualora il computer sia invece acceso e questo vale anche per un dispositivo mobile, affiorano una serie di problematiche circa la ripetibilità in quanto lo spegnimento potrebbe (si usa il condizionale ma trattasi di una probabilità che confina con la certezza) provocare una riscrittura di tutta una serie di informazioni (metadati dei file, riallocazione dei dati sulle memorie e sull' *hard disk*, perdita dati su memoria volatile RAM). In questi casi converrà pensare ad una alimentazione mediante batteria esterna nel caso di un computer o con carica batterie nel caso di *smartphone* o *tablet* considerate le loro limitate capacità di durata.

Ha senso poi considerare un'ulteriore variabile, data dalla modalità di spegnimento del calcolatore, che può avvenire per interruzione improvvisa dell'alimentazione oppure mediante la consueta procedura di arresto prevista dal sistema operativo: nel primo caso alcuni processi[67] vengono chiusi in un certo modo, mentre nel secondo in un altro. In altri termini, sono differenti le tracce lasciate a disposizione degli investigatori.

Può essere altrettanto interessante esaminare nel dettaglio la volatilità dei dati nella memoria, che nello specifico, è la classica situazione che si presenta con lo spegnimento di un computer.

Il processore, la CPU, prima di accedere ai dati controlla un'area di memoria detta cache (disponibile subito e velocemente).

Questo significa che la memoria cache mantiene copie dei dati compresi quelli criptati[68]. Anche da sistema a sistema poi può variare il come le modifiche vengono scritte e cioè se solo nella cache e non nella memoria principale.

Di fatto però spegnendo un sistema i dati della cache che comunque avevano qualche possibilità di essere recuperati vanno sostanzialmente persi. Di qui la previsione di trovarsi nella condizione di un accertamento tecnico irripetibile perché va fatto contestualmente in previsione della possibile perdita dei dati.

---

[67] Qui per processo si intende chiaramente un programma in esecuzione. In un *computer* molti programmi lavoro in background senza che l'utente ne abbia consapevolezza. La loro chiusura improvvisa può riallocare in modo inadeguato dati e talvolta rovinare alcuni processi.

[68] Oltre alla memoria principale, che è pur sempre lenta, esiste anche una memoria *cache*. E' di dimensioni ridotte ma veloce. Questa memoria mantiene una copia dei dati della memoria principale utilizzate più di recente. Cosicché la CPU (processore) prima di accedere alla memoria principale controlla la cache. Se li trova li usa altrimenti torna alla memoria principale (con più lentezza). Quindi, se pur la *cache* scarichi spesso parte di dati, potenzialmente contiene copie di dati segreti.

Volendo ampliare ancora le casistiche tecniche, un cero interesse lo offre inoltre la differenza che può fare un riavvio cosi detto a caldo e a freddo.

Un riavvio a caldo (reset) può non reinizializzare completamente lo stato e pertanto non azzera le impostazioni effettuate dall'utente.

Con certe tipologie di memorie comunque una volta tolta la corrente le informazioni su di esse permangono se la stessa viene raffreddata, ma la cosa non appare già da subito di estrema facilità per varie ragioni.

In generale nei casi di urgenza, dal punto di vista giuridico, conviene pensare di operare in condizioni di irrepetibilità con la conseguenza normativa e giuridica che queste hanno in previsione.

Comunque per rimanere in condizioni di legittimità, anche costituzionale, negli atti non ripetibili bisogna assicurare che i metodi utilizzati negli accertamenti siano affidabili, e vengono utilizzati dei protocolli noti ovvero delle *best practices*, nel rispetto della catena di custodia del reperto.

Riprendendo quanto sopra esposto, e volendo sintetizzare, di norma l'attività di acquisizione di dati da un computer acceso dovrebbe considerarsi un atto di natura irripetibile da compiere nel contraddittorio delle parti.

L'effettuazione di un accertamento tecnico non ripetibile senza il rispetto degli adempimenti di cui all'art. 360 del c.p.p., con i criteri e modalità precedentemente stigmatizzate, comporta la sanzione dell'inutilizzabilità ai fini decisori dei risultati dello stesso. La valutazione di come procedere deve essere fatta prima dell'inizio di ogni operazione in quanto la modificazione dei dati originali è solitamente irrimediabile.

Altro caso di operazione irripetibile è sicuramente il dumping della memoria RAM utile per esempio quando si vogliono trovare delle password ancora residenti in essa[69]. Alle volte è inevitabile agire su questa con strumenti adeguati e rapidi. Vengono solitamente utilizzati in tali occasioni le tecniche di *carving*.

Le tecniche di carving spesso possono essere utilizzate anche quando si vogliono recuperare file cancellati. Anche qui prima che i settori dell'*hard disk* siano riscritti va fatta al più presto l'analisi.

[69] Non si vuole scendere troppo nei dettagli tecnici, ma può succedere che il cosiddetto *file* di *swap* che si estende anche su disco rigido possa contenere ancora preziose informazioni. In pratica la RAM estende la propria capacità su questo partizione di swap del disco. Potrebbe quindi esserci la possibilità che alla riaccensione del *computer* la partizione non sia ancora sovrascritta e quindi avere la fortuna di trovare qualcosa.

.-4 Tecniche utilizzate nell'analisi

Si è visto che la convenzione di Budapest ha avuto un ruolo importante nel definire le metodologie di intervento della *digital forensics* e le cui condizioni essenziali sono l'impiego di procedure scientificamente accettate, determinismo e giusta tempistica delle attività svolte e ripetibilità degli accertamenti tecnici[70]

Le appena citate prescrizioni derivanti dalla convezione di Budapest vogliono significare, anche alla luce di quanto già esposto, che con essa vengono fissate e poste delle basi per operare con modalità tecnico-scientifiche corrette e con delle tempistiche ben determinate.

Con riferimento anche alle leggi scientifiche e alla correlata prova scientifica si ravvisa la necessità che l'attività del tecnico o dell'autorità giudiziaria dovrà essere eseguita con una modalità che sia la più asettica e scientifica possibile, allo scopo di rendere l'operato della ricerca probatoria, la più credibile e affidabile possibile in modo da dover essere ricostruibile. E' chiaro che un comportamento totalmente autonomo e non suffragato da alcuna base teorica – tecnica o scientifica – sarebbe facilmente censurabile in sede di dibattimento processuale.

.-5 Metodi e procedure della *digital forensics*

Si è accennato che la prova informatica [71]è connotata da due caratteristiche specifiche che sono l' immaterialità e la fragilità. Non per nulla i sistemi informatici prevedono procedure di salvataggio (*backup*) e *disaster recovery*[72]. Inoltre da un punto di vista tecnico giuridico l'accensione o lo spegnimento del dispositivo può provocare una perdita dei dati della memoria principale RAM (anche se come visto con tecniche di raffreddamento possano essere ripristinate parte di questi) e la variazione dei metadati (per. es. *timestamp*) dei file.

Diventa evidente quindi la delicatezza della prima fase investigativa dove un comportamento errato può rendere inservibile la prova.

---

[70] Nel senso che, per esempio, la copia clone di un *hard disk* permette la ripetibilità dell'accertamento in quanto è assicurata la riproducibilità di informazioni identiche a quelle contenute nell'originale

[71] Spesso chiamata anche *digital evidence*.

[72] Sono processi di conservazione dell'informazione essenziali nei sistemi informatici. I *back-up* sono piuttosto comuni in tutti i dispositivi e sono ottenuti anche mediante procedure automatizzate su supporti vari quali memorie di massa o nastri ma anche su reti SAN dedicate. La forma di salvataggio legata al *disaster recovery* è propria dei *data cente*r e consiste nella totale replicazione dei dati ad una certa distanza di sicurezza si da contemplare l'ipotesi di grandi disastri come per esempio terremoti.

Con questa breve premessa, peraltro sintesi di concetti già evidenziati, si rappresentano[73] di seguito le fasi procedurali[74] nella formazione della prova digitale.

.....5.1.- Identificazione

Sulla scena del crimine bisogna, innanzi tutto, identificare il dispositivo che può contenere prove (*digital evidences*), per poi acquisirle.

Nel caso in cui il personale incaricato delle indagini si trovasse di fronte un computer converrà (sono misure di massima):

- Controllare lo stato del dispositivo (acceso/spento)
- Se il computer è spento potrà a meno di particolari condizioni essere sequestrato al fine di analizzarlo con dettaglio (configurazione hardware, software, verifica volumi criptati, configurazioni particolari RAID/NAS, BIOS)
- Se proprio deve essere spento conviene staccare la spina e questo eviterà che vengano effettuate dal sistema operativo tutte quelle operazioni di sovrascrittura tipiche di uno spegnimento regolare
- Verificare se ci sono a disposizione backup del sistema
- Acquisire anche qualche foto del sistema e verificare la presenza di connessioni varie (rete locale/rete mobile)
- Descrivere brevemente il locale della scena
- Fare attenzione a non alterare il sistema e qualora si decida per il sequestro fare attenzione al trasporto
- Qualora si acquisiscano solo estrapolazioni parziali calcolare subito i codici di hash

[73] Anche il NIST (National Institute of Standards and Technology) distingue quattro fasi all'interno della *computer forensics*: la raccolta, l'esame, l'analisi, la presentazione, tutte riferite alla prova digitale. La raccolta è data dall' identificazione, etichettatura, registrazione e acquisizione dei dati digitale, nel rispetto di procedure che preservino l'integrità degli stessi. L'esame consiste nel processo di valutazione del dato digitale attraverso metodi automatizzati e manuali che preservino l'integrità del dato digitale l'analisi invece si sostanzia nel processo di verifica dei risultati raggiunti dall'esame dei dati al fini di ottenere le risposte ai quesiti per i quali è stato raccolto ed esaminato il dato digitale stesso. La presentazione dei risultati dell'analisi comprende infine la descrizione delle attività compiute e degli strumenti utilizzati, oltre l'eventuale elencazione delle ulteriori operazioni che sarebbero necessarie per completare l'analisi forense

[74] N. BASSETTI, *Indagini digitali vademecum di uno Sherlock Holmes informatico*, 2011, p.16-55.

.....5.2.- Acquisizione (Analisi e valutazione)

Una volta trovate delle prove bisognerà valutarle e contestualizzarle. Per esempio se si trovano delle immagini pedopornografiche nel *pagefile.sys* oppure nella *cache* del *browser*, questo non implica che l'utente sia passibile di denuncia o che ci si trovi davanti ad una ipotesi di reato ma che o volontariamente o involontariamente ha scaricato delle immagini in maniera automatica

- Fare attenzione a non alterare i dati[75]
- Se un computer ha volumi criptati evitare, anche con sistemi di alimentazione esterna, di spegnerlo
- Annotare la tipologia del sistema operativo
- Annotare i software presenti
- Se il caso filmare le operazioni che si stanno facendo specie se il sistema è acceso
- Se possibile effettuare un dump della RAM
- Scollegarlo alla rete se non serve la connessione

.....5.3.- Presentazione

Tutto deve essere descritto nei minimi particolari in modo semplice e chiaro e deve essere rispettata la catena di custodia. Le prove vanno salvate e conservate su supporti ottici/magnetici e codificate con *hash*[76] e poi creare un file che contiene i codici che a sua volta dovrà essere codificato al fine di non dare la possibilità di alterare le prove con rimasterizzazioni.

---

[75] Corte di Assise di Appello di Milano, Sezione Seconda N. 49/2010 Reg. pag. 14 " Ciò nondimeno, quella preliminare e sommaria attività investigativa effettuata in "totale buona fede" ma con *metodologie scorrette aveva rappresentato una causa di potenziale alterazione e dispersione del contenuto del documento informatico; situazione che poteva aver messo in pericolo la possibilità dell'imputato di provare la fondatezza del proprio alibi. Pertanto il giudice attesa la rilevanza dell'accertamento in esame che involgeva temi probatori di grande rilievo e forse compromessi dalla mancata salvaguardia dell'integrità e della salvaguardia del documento informatico; e tenuto presente il contrasto delle conclusioni dei consulenti delle Parti dispose un accertamento peritale ritenendolo assolutamente necessario ai fini della decisione. Il Collegio peritale accertò che le scorrette condotte di accesso effettuate dai carabinieri avevano effettivamente determinato una sottrazione di contenuto informativo del personal computer dell'imputato pari a 73,8% dei file visibili*". Questo evidenzia l'utilizzo di metodologie, best pratices, inadeguate ai principi della Legge n. 48/2008.

[76] Corte di Cassazione - Sezione II penale - Sentenza 12 dicembre 2008-13 marzo 2009 n. 11135 " L'esperibilità delle procedure di hashing, ossia delle tecniche volte a verificare l'integrità e la conformità all'originale del dato informatico sequestrato e conservato in copia su un apposito supporto (nella specie Cd-Rom), è una questione di merito, potendosi in sede di legittimità esclusivamente delibare se gli accorgimenti adottati dalla polizia giudiziaria delegata siano o meno idonei in astratto a tutelare le finalità indicate dal legislatore negli articoli 247, comma 1-bis, e 354, comma 2, del c.p.p. per come modificati dalla legge 48/2008 di ratifica della Convenzione del Consiglio d'Europa sul cybercrime". L'esperibilità della procedura di hashing valutabile solo in sede di merito.

.-6 Strumenti informatici e software comunemente utilizzati

I *tools* per l'analisi forense sono vari[77]:

.....6.1.- Sistemi virtuali

In questi ultimi anni i sistemi di virtualizzazione hanno preso sempre più piede. Le macchine virtuali, gli oggetti di tali sistemi, sono replicabili infinitamente nell'ambiente virtuale nel senso che possono riprodurre emulandolo un sistema informatico nella sua interezza hardware e software. La cosa è piuttosto interessante specie quando si vuole cercare un particolare comportamento di una macchina oggetto di indagine o di simularne alcuni aspetti. Gli stati della macchina virtuali sono poi "solidificati" attraverso funzioni cosi dette di *snapshot*.

Tali sistemi rappresentano insomma una sorta di copia integrale del *device* sotto indagine. È sempre più frequente inoltre che siano gli stessi soggetti ad utilizzare delle macchine virtuali e quindi appare inevitabile clonare un tal sistema. Inoltre bisogna prestare attenzione al fatto che le macchine virtuali possono essere chiuse senza salvare lo stato. Solitamente dei file di log certificano ogni modificazione della macchina.

I prodotti a disposizione per creare un ambiente virtuale sono molteplici e vanno dai prodotti commerciali a quelli *open source.*

.....6.2.- Programmi di hacking o cracking

Si è accennato in precedenza che il più delle volte i sistemi o i *device* sono protetti da password e spesso integralmente o parzialmente possono essere crittografati. La crittografia complica notevolmente la vita all'analisi dei sistemi e quindi talvolta si devono utilizzare programmi di *brute force*[78] con il chiaro intento di forzare il sistema. Nei casi più difficili i tempi possono allungarsi notevolmente.

Talvolta in casi estremi bisogna ricorrere a sistemi di *debugging* e *dissasembling* per l'analisi del codice.

---

[77] A. GIRARDINI, G. FAGGIOLI, *Digital Forensics*, *cit.,* pp. 238-243.

[78] Esistono vari tipi di "attacchi contro gli schemi di cifratura. Un attacco di tipo dizionario che prova ad utilizzare ogni possibile combinazione di caratteri viene chiamato attacco esaustivo di tipo forza bruta.

.....6.3.- Programmi di conversione

Alcuni formati, qui si parla di estensione dei file, sono legati anche a programmi proprietari e dei quali non si può pensare di possederli tutti.

.....6.4.- Programmi di file analysis

Con questi programmi si intendono analizzatori di file per vederne dati e metadati. Non è infrequente, per le più varie ragioni, che alcuni file vengano rinominati con estensioni diverse[79] da quelle originali. Si pensi anche a delle tentate alterazioni[80] di particolari presenti in una foto digitale.

.....6.5.- Programmi di data e file recovery (carving)

Sono programmi che tendono al recupero dei file, directory, che sono stati cancellati o rovinati per svariate ragioni anche fraudolente con l'intento cioè di eliminare tracce che possano portare a evidenze digitali talvolta compromettenti. Sono software che non sempre riescono nella loro intenzione. Spesso comunque, nelle foto ad esempio, si ottengono risultati parziali.

.....6.6.- Caratteristiche dei programmi più idonei

In questa sede non è interesse di fare nomi dei software più comuni ma quello che può interessare è che siano multipiattaforma[81] e che siano o commerciali e quindi *closed* o *opensource* e cioè a codice sorgente "libero". La cosa può avere interesse anche in sede processuale perché potrebbe essere eccepito il fatto di non fidarsi completamente del loro funzionamento.

Allo scopo esistono diverse soluzioni *software* (e *hardware*) che aiutano l'investigatore ma un argomento interessante che riguarda i *software* da utilizzare e che spesso

[79] Si supponga di avere una documento word del tipo documento.doc e che sia invece stato rinominato come documento.jpg potendosi quindi confondere con una foto.
[80] Le foto digitali possono essere sicuramente alterate con aggiunta o sottrazioni di parti come alla "rimozione" di dettagli utili alle indagini. Inoltre possono nascondere informazioni, cosa di cui si occupa la steganografia.
[81] Vadano bene cioè per diversi sistemi operativi.

viene posto è sulla loro natura commerciale o *open source*. La cosa infatti potrebbe comportare contestazioni in ambito processuale. Il *software* commerciale è infatti un prodotto "chiuso" nel senso che il codice non è disponibile per essere esaminato, mentre quello *open source* è "aperto" e quindi disponibile a essere analizzato. La questione che potrebbe porsi è quindi quella di capire se con un software proprietario potrebbe venire meno l'attendibilità della fonte di prova. Questo normalmente non avviene anche perché i software commerciali più noti sono riconosciuti come validi e comunque spetterebbe al difensore o al giudice argomentare con motivazioni valide l'eventuale inattendibilità invocando se il caso l'art. 189 del c.p.p. per individuare quali dati siano eventualmente inaffidabili[82].

Non si ritiene il caso di elencare i software disponibili anche perché non ha un grande rilievo in questo contesto. Ciò che però può essere interessante è di elencare con una certa sintesi le funzioni che in generale un pacchetto software del genere può fare[83]:

- Funzioni di *cloning* e *imaging*
- Supporta i principali formati immagine della digital forensics
- Supporta i più noti hypervisor (macchine virtuali)
- Supporta i dischi RAID
- Identifica automaticamente le partizioni perse o cancellate
- Analisi e dump della RAM
- Creazione di cataloghi file e directory per i media acquisiti
- Supporta gran parte dei file *system*
- Algoritmi di hashing
- Ricerca fisica e logica
- Funziona senza installazione
- Salva fonti di prova in cartelle dove i file sono copiati mantenendo inalterati i metadati rispetto alla loro posizione originaria
- Gestione read-only (sola lettura) fonti di prova digitali
- Sistema di carving
- Visualizza 270 tipi di file
- Ricerca metadati in quantità enormi di estensioni di file
- Interpreta email più note

[82] D'AIUTO G., LEVITA L., *I reati informatici disciplina sostanziale e questioni processuali*, **cit**., p.124-125
[83] X-Way Forensic - http://www.x-ways.net/forensics/

- Sistema di identificazione file crittografati[84]
- Algoritmo per la ricerca del colore della pelle all'interno delle fotografie
- Può estrarre dai file video immagini a intervalli regolari

Si sono volutamente omesse molte altre funzioni perché squisitamente tecniche e meno apprezzabili in questo contesto. Quelle riportate però sono significative e danno una idea concreta a quella che sono le funzioni automatizzate che si riescono a ottenere con i software in circolazione.

.-7 Problematiche relative alla copia forense

Si è già affrontato in precedenza il problema della copia dei dati portando alla luce alcune problematiche collegate all'esatta corrispondenza della copia rispetto all'originale. Uno dei problemi è che in questi anni il progresso tecnologico ha fatto nel versante delle memorie di massa importanti passi aventi specie nelle dimensioni di questi supporti.

Si è già evidenziato che la copia forense deve essere tale da copiare tutte le informazioni presenti nel supporto oggetto di indagine. Questo comporta che andranno copiate per intero le strutture del *file system* come il *master boot record*[85], la tabella delle partizioni, i metadati e lo spazio non allocato e spesso si è anche in presenza di partizioni del disco di sistema nascoste.

Le grandezze degli *hard disk* hanno raggiunto capacità di Terabyte il che comporta grosse difficoltà nel copiarle anche se il mercato attuale propone interfacce con velocità e capacità maggiori rispetto al 2008. Inoltre è ormai tipico di molte realtà di disporre di unità NAS (per non parlare delle reti SAN) con i dischi configurati nei modi più disparati e con tecnologia RAID[86].

Inoltre in alcune situazioni i sistemi in esame possono porre seri problemi nel caso in cui dovessero essere spenti, come i *data center*. Un primo problema potrebbe essere quello di

[84] La crittazione di un supporto informatico costituisce una eventualità che rende le operazioni notevolmente più complesse. Se il *computer* non è spento e si ha il sentore che il sistema, o parte di esso, sia crittografato converrà porre notevole attenzione. La ricerca delle chiavi può essere assai laborioso e con risultati non sempre garantiti in particolare se queste sono robuste.

[85] Il *master boot record* (MBR) è quella parte di disco, meglio settore, dedicata all'avvio del sistema operativo. Infatti l'HDD è suddiviso in partizioni (primarie e logiche) e il *master boot record* gestisce la tabella delle partizioni per decidere quale sistema operativo far partire. In sostanza qui si vuole dire che il disco deve essere copiato nella sua totalità.

[86] *Redundant Array of Inexpensive Disks* è una configurazione particolare degli hard disk tale da offrire maggior sicurezza e resistenza ai faultollerance. Le difficoltà si possono trovare perché alle volte queste configurazione sono gestite dal sistema operativo e altre da soluzione proprietarie sia a livello di software che di hardware.

tipo pratico ed economico che uno spegnimento di una tale struttura, attiva 24 ore su 24 ogni giorno, porrebbe. Nel caso di un sequestro inoltre l'estrazione dei dati richiederebbe tempi lunghi e potrebbe essere necessario nominare un custode giudiziale.

Anche i nuovi dischi SSD possono presentare qualche difficoltà nella loro analisi. I dischi allo stato solido subiscono il fenomeno del deterioramento, ossia quando si cancella un file, il comando TRIM del sistema operativo dice al *controller* del disco di cancellarlo[87]. Poiché gli SSD seguono una regola particolare e per cancellare un file devono prima scrivere, le operazioni di cancellazione non sono in tempo reale, ma in background e gestite dal controller, poi una volta cancellati i blocchi, non si recupera più il *file*, poiché sovrascritto.

Quindi, quando si stacca un SSD[88] e lo si attacca ad un altro computer, il *write blocker* non blocca il deterioramento, dato che il fenomeno si attiva dall'interno, appena il *controller* riceve corrente elettrica.

L'unico sistema per elidere questo problema è quello di effettuare il dissaldamento dei chip di memoria del disco ed il conseguente *dump*[89], con tutta la difficoltà che ne deriva, sia tecnica sia di ricostruzione dei dati.

Altro problema nella copiatura si è detto è quello di non alterare il sistema dal quale si vogliono acquisire i dati. Nella stragrande maggioranza dei casi i sistemi operativi "annotano" marcando al loro interno il supporto ad esso collegato. Questo avviene perché il sistema ha bisogno di riconoscerlo. Dopodiché avvengono tutta una serie di scritture tra i dispositivi che vanno ad inficiare la genuinità delle operazioni.

In soccorso i tecnici hanno degli apparecchi specifici chiamati blocker. Questi dispositivi hardware impediscono qualsiasi scrittura sul disco collegato evitando che il sistema operativo del computer esaminato "sporchi", così in gergo tecnico con dati e metadati il supporto di copiatura.

---

[87] Il discorso può essere complicato perché la cancellazione dei *file* in un hard disk è di solito logica fino a che i suoi settori non vengono sovrascritti

[88] Unità a stato solido o drive a stato solido Solid State Drive

[89] Dump della memoria è una copia di quanto in RAM. Il *dump* della Ram (esistono per precisione più dump della RAM) è un sorta di copia integrale della memoria (al pari della *bit stream image* delle memorie di massa) e possono distinguersi perché non tutti i *dump* contengono i registri e lo stato del processore. Dissaldando il chip di memoria le cose naturalmente si possono complicare in una situazione già complicata di per se.

.-8 Questioni relative ai supporti di memorizzazione

Un fatto da non sottovalutare è inoltre quello di preservare lo stato della prova. Infatti con alle modifiche apportate con la Legge n.48/2008 agli artt. 244 e 247 del c.p.p. si è posta molta attenzione alla conservazione dei dati originali si da impedirne l'alterazione.

La cosa assume ancora maggiore valenza nel caso degli accertamenti tecnici ripetibili di cui all'art. 359 del c.p.p.

In linea generale non tutti i supporti presentano le stesse caratteristiche in termini quantitativi (si pensi alle grandi quantità di dati in cui un operatore può imbattersi) e qualitativi, anche per quanto riguarda la durata nel tempo e il fatto che siano modificabili o meno. Converrà comunque prevederne più copie.

.....8.1.- Supporti magnetici

Qualunque sia il supporto magnetico utilizzato, nastro magnetico o *hard disk* tradizionale dovrà comunque essere riposta la massima cura per la loro protezioni contro urti e campi magnetici. Buona norma è poi quella di catalogarli bene con una sintetica ma efficace descrizione.

.....8.2.- Supporti ottici

Qui si ritrovano i CD R/RW-DVD+-R/RW – BlueRay supporti che però sono molto sensibili alla luce e al calore. Inoltre alcuni se non sono chiusi in sessione possono essere ancora alterabili. Anche qui vale la regola di una catalogazione e protezione.

.-9 Il problema della definizione della cronologia degli eventi (la c.d. “timeline”)

La riconducibilità di un determinato fatto all’interno di un preciso spazio temporale è, senza ombra di dubbio, uno degli elementi primari per la corretta interpretazione della scena del “crimine”, in quanto consente di rivelare la dinamica degli eventi nell’ordine in cui essi si sono verificati. La ricostruzione della sequenza temporale degli eventi che hanno determinato un fatto è infatti d’interesse vitale per la risoluzione di qualsiasi caso, di natura legale o professionale, indipendentemente dal contesto di riferimento.

Uno degli strumenti che consentono di effettuare l'analisi forense sul tempo è la cosiddetta *timeline*, termine con il quale nell'informatica forense si indica la cronologia di tutti gli eventi registrati in un determinato periodo nel sistema analizzato. Avere dei punti di riferimento temporali aiuta sia la ricerca che l'analisi delle informazioni e riduce significativamente il numero di ipotesi che si possono formulare durante lo svolgimento delle indagini preliminari.

Di seguito si prendono in considerazione due dei principali strumenti per definire una timeline, i *log*s e il *timestamp*.

.....9.1.- I files di log

Tutti i sistemi informatici generano file di log, ovvero registrazioni che tracciano nel tempo con una sequenza ordinata ogni azione di ogni processo in esecuzione. Normalmente molti processi lavorano in background all' insaputa dell'utente e monitorano le sue azioni dalle più comuni quali quelle di accesso al sistema a quelle di interazione con esso. Alcuni di questi file di log sono gestibili solo da amministratori dei sistemi mentre altri sono propri delle applicazioni software e non godono di particolari requisiti di sicurezza. Naturalmente alcuni di questi file sono come per esempio nel caso di servizi forniti da provider di proprietà di questi a cui vanno eventualmente richiesti (si pensi all'accesso alla rete, posta elettronica, chat).

Il primo e più importante elemento per definire una timeline, è dato appunto dai *files* di log. Infatti i *file* di log rappresentano un efficace indice perché agevola la ricostruzione delle azioni che un soggetto compie all'interno del suo sistema informatico ed è fonte d'informazione per l'analisi a posteriori di un evento.

.....9.2.- Il timestamp

Oltre ai file di *log* possono essere utilizzate delle informazioni cronologiche associate ai singoli *files*, dette *timestamp*. Le informazioni di *timestamp* marcano solamente l'orario dell'ultima operazione eseguita su un determinato file e possono essere una valida fonte di prova quando rimangono poche alternative.

L' analisi del *timestamp*, tuttavia, non è semplice, soprattutto in caso di grandi quantità di dati.

Affinchè un *timestamp* registrato in un sistema di calcolo possa essere sostenuto quale elemento di prova di un'indagine forense, deve essere preso in considerazione alcuni fattori problematici:

- il tempo in un sistema di calcolo è scandito dall'orologio[90] *hardware* del sistema e, in alcuni casi, da un ulteriore *software* di gestione del clock (Server NTP[91]);

- l'orario del sistema può differire in maniera considerevole dall'ora reale in quanto può essere configurato per una *time zone* (fuso orario) diversa o può essere mal impostato;

- l'orologio può essere manipolato facilmente;

- un orologio può essere eseguito più velocemente o lentamente rispetto al tempo standard.

.-10 Conclusione

La *digital forensics*, alla luce della legge 48/2008, si può intendere anche, con una definizione diversa da quella dell'introduzione, come quell'insieme di attività volte alla preservazione, ricerca, identificazione e analisi delle prove informatiche.

Per parlare con maggiore cognizione di *digital forensics* è stato necessario delineare, a grandi linee, l'architettura di un elaboratore introducendo, se pur con le generalità del caso, alcuni elementi tecnici circa le sue componenti hardware e software. In tale contesto si sono considerate, perché di particolare interesse, le memorie dei dispositivi elettronici e il sistema operativo.

Poste queste premesse tecnologiche si è poi affrontato il problema dell'analisi dei sistemi informatici.

Con lo sguardo rivolto al codice di procedura penale, così come modificato dalla legge n. 48/2008 circa le indagini informatiche, si sono affrontate le problematiche mediamente riscontrabili alla sua applicazione concreta.

A riguardo, e tenendo ben presente il principio della non alterazione del dato digitale originale, è venuto in rilievo il problema dell'accertamento tecnico ripetibile e irripetibile.

---

[90] In un *computer* vi sono un orologio hardware e uno software. Il primo è funzionante grazie ad una batteria motivo per cui funziona anche se il *computer* è non alimentato. L'altro invece funziona solo con il *computer* acceso. Se pur esiste tra di loro una sincronizzazione, di fatto sono spesso disallineati. Dal punto di vista tecnico entrambi gli orologi presentano degli inconvenienti.

[91] Network Time Protocollo. L'orologio non è unico e questo può creare problemi nelle indagini.

La questione non è di poco conto, anche perché non esiste una linea netta di demarcazione che dia una certa sicurezza nel modus operandi da tenersi dai vari operatori tecnici né una casistica ben definita e esaustiva delle problematiche riscontrabili.

Quello che è certo è che bisogna necessariamente valutare il caso che si ha davanti con attenzione. Alcune sentenze che danno comunque delle indicazioni anche di rilievo non esauriscono di certo la questione.

Anche alla luce degli articoli legati agli accertamenti tecnici si sono evidenziate con alcuni esempi le incertezze che si possono prospettare.

Si è avuto modo inoltre di argomentare sulle metodologie ormai standard relative alle fasi principali delle indagini informatiche ‑in un sistema informatico come l'identificazione, l'acquisizione, la presentazione. Fasi assai delicate che vanno svolte con cura e documentate nei passaggi.

Lo sguardo è stato rivolto anche ai *tool* e *software* usati analizzandone anche concretamente in alcuni casi le funzionalità.

Con attenzione si è considerata la questione relativa alla copia dei dati originali si da preservarne lo stato originario e le modalità di certificazione della stessa. Uno sguardo rapido si è rivolto anche al supporto dove custodire la copia, questione non banale e scontata. Si ricorda infatti che le prove permangono in questi supporti a disposizione di ogni esigenza processuale e ogni sede processuale può giovarsene.

Una questione molto delicata è data dalla *timeline*, la riconducibilità di un determinato fatto in un preciso spazio temporale. Gli orologi interni ad un computer sono più di uno e non sempre in sintonia. Non solo essi sono manipolabili, ma è difficile capire se ciò sia avvenuto per un evento casuale, per colpa o per dolo dell'utente.

CAPITOLO III.- IL SEQUESTRO E L'ANALISI DI DISPOSITIVI MOBILI

.-1 Introduzione

La *mobile forensics* ha per oggetto i dispositivi mobili che, come precedentemente evidenziato, rappresentano una classe in continua evoluzione per tipologia e caratteristiche. Tra di essi rientrano certamente a pieno titolo, se così si può dire, gli *smartphone* e i *tablet*, questi ultimi spesso dotati di moduli di comunicazione cellulare e quindi per certi versi simili ai primi[92]. Infatti, gli *smartphone* in particolare sono riconducibili tecnicamente a dei computer (talvolta anche assai potenti dal punto di vista elaborativo e prestazionale) che inglobano dei moduli di comunicazione cellulare e *wireless* e moduli di espansione per schede di memorie di massa esterne. Essi sono e possono essere fonte di prova per le chiamate effettuate, i contatti contenuti, i messaggi (sms, mms, messaggi di altra natura), foto, video, audio, localizzazioni di posizione (Global Positioning System).

Di seguito si prendono in considerazione gli aspetti specifici che riguardano l'analisi delle informazioni contenute negli *smartphone*. Altre questioni sono riconducibili tendenzialmente alla *computer forensics*.

.-2 Breve premessa sul funzionamento dei *mobile devices*

Converrà introdurre qualche spiegazione anche di tipo tecnico sulla telefonia cellulare allo scopo di comprendere meglio le problematiche che li possono contraddistinguere nell'acquisizione delle prove rispetto alle altre apparecchiature informatiche.

La telefonia cellulare è una tipologia di accesso ad una rete telefonica realizzata per mezzo di onde radio e il termine cellulare si riferisce al fatto che l'utilizzo del sistema di comunicazione senza fili utilizzato suddivide le grandi aree geografiche in aree più piccole chiamate celle.

[92]Le analisi compiute di seguito sono condotte da un punto di vista generale; come è noto, il mercato fornisce una estrema varietà di modelli con funzionalità molto eterogenee.

Prima di proseguire è utile considerare che i telefoni cellulari vengono suddivisi dal NIST[93] (*National Institute of Standards and Technology*) in tre categorie[94] così sinteticamente individuabili:

- **Basic Phone**: terminale radiomobile con velocità di calcolo e memoria limitata privo di scheda di memoria aggiuntiva;
- **Advanced Phone**: terminale radiomobile con velocità di calcolo e memoria superiore con scheda di memoria aggiuntiva;
- **Smart Phone**: terminale radiomobile con elevata capacità di calcolo, memoria esterna, periferiche *wireless* e porte di comunicazione di varia natura.

I *mobile device* più avanzati sono tecnicamente dei terminali radiomobili che, nella loro architettura di sistema, assomigliano molto a dei computer e sono quindi dotati di schermo, processore, memoria principale e di massa – taluni anche di una memoria esterna su scheda SD o microSD – una o più fotocamere, una tastiera, porte di ingresso e uscita, moduli wireless (wifi, bluetooth, infrarossi, nfc) e una batteria piuttosto complessi.

Le memorie dei mobile device giocano un ruolo importante. Le memorie interne non volatili normalmente sono dei due tipi indicati NAND o NOR e si distinguono in termini di velocità e capacità. La RAM è una memoria, come si è detto, di tipo volatile dove "girano" i programmi in esecuzione (esistono comunque dei tool per catturare i dati in esecuzione).

Per accedere alla rete cellulare, GSM[95], UMTS[96] o LTE[97] che sia, questi dispositivi contengono, in apposito modulo dedicato una particolare smart card detta SIM[98] o USIM[99]. La scheda servirà al radiomobile per autenticarsi e connettersi alla rete cellulare. Per inciso anche la smart card è un dispositivo dotato di una struttura tutta propria (file system, memoria, coprocessori).

Con queste dovute premesse si possono ora, individuare sicuramente quattro aree di interesse ai fini probatori che sono rappresentate da:

- una memoria interna
- una memoria di massa o rimovibile aggiuntiva

[93] http://www.nist.gov/
[94] http://csrc.nist.gov/publications/PubsSPs.html#800-101
[95] Global System for Mobile Communications.
[96] Universal Mobile Telecommunications System.
[97] Long Term Evolution.
[98] Subscriber Identify Module.
[99] Universal Subscriber Identity Module

- la scheda SIM
- il provider di telefonia mobile[100]

in effetti quello che interessa invece in questo contesto, a livello di analisi probatorie del dispositivo mobile, e quello di estrarre le attività che il telefono cellulare ha svolto nel tempo di interesse all'indagine. Come si è sopra dato cenno questi dispositivi contengono, all'interno delle loro memorie, molte informazioni di messaggistica (sms, mms, *email*) contatti, documenti, foto, video, posizionamenti (gps) , che possono costituire fonti di prova di un certo interesse.

Il maggior interesse e la maggiore difficoltà nella *mobile forensics*, come si è già considerato in generale per gli altri sistemi, è quello di recuperare i dati nelle memorie interne di questi dispositivi. Questi possono essere per esempio l'identificativo IMEI[101], data e ora, lingua utilizzata, rubrica, immagini, chiamate effettuate, ricevute e perse, le note, gli (M)SMS, le email, e i "log" del GPS.

Gli strumenti a disposizione degli inquirenti per l'analisi delle memorie interne dipendono anche dal sistema operativo utilizzato dallo *smartphone*. Il sistema operativo risiede in una memoria di tipo NAND o NOR e tipicamente l'esecuzione del codice avviene in RAM. Gli attuali sistemi operativi in commercio si possano raggruppare in quattro grandi famiglie:

- Android (ecosistema Google)
- iOS (piattaforma Apple)
- Windowsphone (sistema operativo Windows)
- Blackberry (piattaforma RIM)

Naturalmente non sempre è facile possedere gli strumenti tecnici hardware e software per analizzare tutti i telefoni cellulari. In verità il discorso vale per tutti i *mobile device* in generale, ma in particolare quando sono il prodotto di soluzioni commerciali proprietarie note come *embedded*.

Questo è un fattore piuttosto importante e di supporto nelle indagini perché per tutti questi sistemi esistono vari tool commerciali o meno con i quali operare.

[100] In questo ultimo caso si può parlare di *Network Forensics*, intendendo con tale espressione l'attività investigativa concernente la telematica e quindi indirizzata nei confronti del provider. Per acquisire questi tipi di dati normalmente vengono richiesti tabulati del traffico telefonico tramite richiesta delle autorità giudiziaria. In questa sede non sarà analizzata per la specificità delle questioni ad essa inerenti.

[101] International Mobile Equipment Identity – E' un codice che lo identifica a livello internazionale. Non è troppo complicato modificarlo.

Per sistemi *embedded,* sono intesi quei dispositivi creati per una determinata applicazione e supportati da una piattaforma *hardware* - *software* proprietaria e che non sempre si relazionano facilmente con gli altri sistemi e dispositivi informatici. Il più delle volte non esistono *tool* specifici e quindi bisogna capire, per facilitarsi le cose al fini di procedere in qualche modo nell'analisi del dispositivo, se comunque sono sistemi derivati da altri noti (e spesso lo sono per il semplice fatto che magari usano sistemi operativi derivati da quelli noti) e di conseguenza procedere con le metodologie conosciute (una sorta di procedimento per similitudine). Questo ben inteso è valido quando si intende lavorare a livello logico, mentre per le memorie di massa estraibili normalmente i dati hanno estensioni note[102].

Bisogna a riguardo premettere che il recupero dati dalle memorie interne è legato talvolta ai software proprietari del produttore e che possono interessare anche il *file system* legato a questo, perché ne è componente e al sistema operativo che è la struttura software principale. Fortunatamente negli ultimi anni, come premesso, si sono delineati pochi ma importanti operatori e ciò ha aiutato l'analisi dei dispositivi, con materiale informativo, e *tools* software adeguati.

Altra cosa importante è poi distinguere le memorie e considerare che una di essa è spesso interna al dispositivo se non l'unica visto che in alcuni casi non esistono slot di espansione. In questo caso, la memoria non potendo essere estratta (andrebbe dissaldata) deve essere letta nella così detta modalità logica con apposito software. Nel caso della estrazione fisica vanno utilizzate apparecchiature dedicate.

Anche la carta SIM, che permette di identificare l'abbonato nella rete, contiene un certo numero di file dai quali è possibile ricavare informazioni relative all'utente:

- International Mobile Subscriber Identity (IMSI);
- preferenze di lingua e di rete (provider di servizi);
- contatori di costi e durata chiamate;
- informazioni circa la corrente (o la più recente) posizione del telefono;
- rubrica;
- messaggi SMS inviati e ricevuti;
- ultimi numeri chiamati.

[102] Le foto per esempio avranno comunque una estensione tradizionale. Stesso dicasi per i filmati. Il *file system* generalmente ricalca derivati linux.

La scheda SIM pone dei problemi. Normalmente in essa sono attivati dei meccanismi di sicurezza come il codice PIN (Personal Identification Number) che va digitato all'accensione (o reset del dispositivo). In linea di massima il sistema operativo ne concede l'inserimento non più di tre volte dopodiché il sistema viene bloccato e deve essere, attraverso il codice PUK, sbloccato[103] (a meno di On the Practicability of Cold Boot Attacks).

Per quanto riguarda invece l'analisi delle memoria esterna le metodologie da adottarsi sono le stesse utilizzate con gli altri dispositivi.

.-3 Problematiche legate alle analisi

Difficilmente agli *smartphone* potranno applicarsi in toto le best practices utilizzate nella "classica" *digital forensics*. Ciò è causato dal fatto che in alcune situazioni, anche se attualmente sempre più residuali, ci si può trovare davanti a dispositivi con soluzioni proprietarie (*embededd*) dedicate e con hardware o software creati ad hoc e di conseguenza con *file system* (organizzazione dei file) anche questi di natura proprietaria. Questo complica non di poco l'estrazione dei dati dalla memoria interna è la possibilità di potere fare una copia *bit per bit* come richiesto dalla prassi.

Comunque, a parte questi casi sempre più residuali, l'approccio può essere duplice:

- Quello di tipo logico, collegando il dispositivo al computer, e lavorando con del software dedicato in modo tale da procedere all'estrazione di file o record. È una soluzione che non permette di estrarre lo spazio non allocato e non si avrà quindi una *bit stream image* come invece si vorrebbe. E' utile ricordare infatti che la copia informatica deve essere un esatto clone dell'originale e questo significa che deve comprendere tutto lo spazio allocato o meno della memoria.
- Quello fisico, che prevede l'estrazione fisica della memoria e leggerla con dispositivi dedicati. L'operazione non è sempre semplice e potrebbe rovinare la memoria stessa e il dispositivo.

In questi casi, anche se non rientrano nelle *best practices* di informatica forense le capacità dell'operatore (perito, consulente) possono essere determinanti.

[103] Esiste qualche tecnica piuttosto complicata per il recupero del PIN.

Considerato la delicatezza dell'analisi del telefono cellulare è importante cristallizzare la situazione e lo stato al momento dell'indagine. Potranno allo scopo essere utile anche documentare mediante foto la scena del rinvenimento del dispositivo oltre che annotare lo stato fisico dello stesso (integrità dello schermo, se acceso o spento) oltre che se necessario video riprendere l'ambiente circostante.

Utile sarà inoltre sequestrare, se li si ritrovano, cavi e caricabatterie, memorie di massa e documentazione ad esso associati.

Ma il problema principale per l'investigatore è quello di isolare il telefono dalla rete cellulare in quanto si potrebbero effettuare sovrascritture generate da informazioni provenienti da parte della rete. L'isolamento della rete si può effettuare in diversi modi spegnendolo (e si potrebbe incorrere in rischi ben più gravi), mettendolo in modalità aereo, utilizzando uno *jammer device*[104], o ponendolo in un contenitore schermato. Infine se ciò non bastasse, richiedendo il blocco al provider, ma è una soluzione che presenta i suoi tempi. Tutte queste possibili soluzioni, come è ovvio pensare, presentano vantaggi e svantaggi.

Senza entrare in dettagli e tecnicismi troppo specifici, si può comunque affermare che lo *jammer* e il contenitore schermato (gabbia di Faraday) sono i più usati e sicuri. Il contenitore ha lo svantaggio di far consumare un po' le batterie cosa di cui si dovrà tenere conto.

Un' ottima alternativa è lo schermare uno spazio intero, con un locale dedicato, per procedere con più facilità all'analisi. Altrimenti si lavorerà in condizioni di maggiore difficoltà come nel caso della schermatura locale del dispositivo, dovendo fare attenzione ad esempio che i cavi utilizzati non facciano da antenna.

Si nota quindi una intrinseca difficoltà di azione a cui si aggiunge il fatto che spesso non ci sono tempi molto ampi di decisione.

Per recuperare informazioni dalla SIM in alcuni casi è uso clonarla e utilizzare questa "copia" per le investigazioni del caso. Dalla SIM originale poi si potrebbero ricavare ulteriori dati.

Con la scheda clonata verrebbero meno i problemi di inserimento del PIN (a cui sono attributi normalmente i famosi tre tentativi).

Inoltre attenzione va fatta alle connessioni *wireless* presenti che vanno usate, se il caso, con attenzione.

[104] È un disturbatore di segnale. Questa apparecchiatura emette un segnale più forte di quello supportato dal cellulare e quindi crea una grossa interferenza

Durante il sequestro è importante anche che non si scarichi la batteria il che potrebbe far perdere data e ora.

Adottati questi accorgimenti si può passare all'analisi del *mobile device* con opportuni software forensi o con hardware dedicati[105].

Si ritornerà poi con più dettaglio sul software da utilizzare mentre invece ecco alcuni esempi di hardware dedicato[106] che a titolo esemplificativo si riportano:

- Cellbrite UFED

- Micro Systemation XRY

- CellDEK

- ED Touch Ultimate

.....3.1.- Il problema del rinvenimento del telefono acceso o spento

Si è già affrontato nel capitolo riservato alla *digital forensics* la problematica relativa allo spegnimento o meno di un sistema informatico qualora trovato acceso. Se nella *computer forensics* questo rappresenta un problema la cosa assume ancora più rilevo nella *mobile forensic* ovvero quando il discorso è legato ai dispositivi mobili cellulari. In particolar modo perché è fondamentale l'isolamento dalle rete e l'attivazione di codici di autenticazione.

I dispositivi accesi o spenti definiscono procedure particolari[107].

- Telefono spento

- analisi esterna all'ambiente e documentale del telefono
- rimozione della SIM
- Analisi della SIM e tentare di recuperare le informazioni
- recupero della rubrica telefonica nella SIM

[105]http://lang.cellebrite.com/it/mobile-forensics/products/standalone/ufed-touch-ultimate - http://www.logicube.com/knowledge/celldek-tek - https://www.msab.com/

[106] http:/lang.cellebrite.com/it/mobile-forensics/products/standalone/ufed-touch-ultimate
https://www.msab.com/
http://www.logicube.com/knowledge/celldek-tek

[107] Alcune volte i tecnici definiscono per i sistemi spenti l'analisi come *post mortem forensics* e per quelli accesi *live forensics*

- recupero dei messaggi dalla SIM
- rimozione della memoria rimovibile inserita nell'apposito slot e l'analisi con i software forensi a disposizione facendo attenzione a non sovrascrivere
- clonazione nel dubbio della SIM
- isolamento del telefono dalla rete mobile
- alimentazione del telefono
- collegamento del telefono al computer e il recupero dei dati memoria principale

- Telefono acceso

- alimentazione del telefono
- estrazione in ambiente schermato delle informazioni
- Analisi SIM e memoria rimovibile
- fare attenzione che se lo spegnimento potrebbe essere richiesto inserimento PIN
- acquisizione della documentazione di funzionamento e uso per procedere anche manualmente all'estrazione dei dati filmando le operazioni e cercando il minor impatto possibile a livello modificativo dei dati
- il desoldering della memoria flash ad avviso anche di chi scrive dovrebbe essere l'ultima alternativa da effettuare. Per la lettura richiede strumenti costosi e le informazioni ricavabili sono parziali.

- Software

Esistono al riguardo molte tipologie di software e chiaramente si distinguono per funzioni e caratteristiche. Vi sono alcuni hardware dedicati che permettono l'acquisizione degli screenshot dello *smartphone*/celluare che sia. Alcuni tool sono dedicati all'analisi della SIM.

Anche in questo caso siamo in presenza di software commerciali e software *open source* e il discorso su questo punto è già stato affrontato nella parte relativa alla *digital forensics*.

.....3.2.- Problematiche più comuni

Si è già avuto modo di incontrare nel corso del capitolo alcune problematiche che contraddistinguono la *mobile forensics* rispetto alle altre.

La cosa più complicata è sostanzialmente quella di effettuare una copia bit a bit della memoria. Si ha talvolta, specie nell'analisi logica, una limitata possibilità di analisi dei dati, estraibili con i tool a disposizione, e purtroppo anche una potenziale irrepetibilità della prova per gli effetti descritti anche in relazione alla modificabilità degli stessi che non è sempre nota. Ogni accesso al dispositivo, ovvero alla sua memoria principale, inevitabilmente comporta modifiche al sistema. Si ricorda infatti che la memoria di cui si parla è la memoria interna del sistema[108].

Il telefono cellulare, si è detto, è sempre soggetto a scambi di informazione con la rete mobile e, se non disattivata, anche con la rete dati Internet. Spesso gli *smartphone* vengono definiti terminali always-on perché sempre connessi. Si pensi anche solo alle cosiddette APP[109], che sono dei pacchetti *software* che una volta installati sul proprio *smartphone* pongono seri problemi non solo alla riservatezza ma anche al potenziale uso delle risorse del telefono. Queste infatti si aggiornano spesso e automaticamente, interagendo con le memorie così da modificarne il loro stato.

Ma non basta perché questi dispositivi fanno ricorso sempre più spesso al *cloud computing* (risorse back-end) e quindi aprono problematiche nuove e diverse da trattare diversamente e con metodologie differenti.

Gli *smartphone* sono oramai gestibili anche da remoto attraverso Internet, nel senso che è possibile installare e rimuovere su di loro applicazioni software o peggio ancora, ovviamente per le analisi forensi, di bloccarlo o di effettuare un wipe delle informazioni senza aggiungere software (un sostanziale reset).

A questi si aggiungono i servizi automatici di aggiornamento del sistema.

Blackberry inoltre non viene riconosciuto né per il suo numero di telefono né per l'IP assegnato[110].

[108] Non esiste qui un write blocker per tali memorie anche perché non si saprebbe come interfacciarsi.
[109] Applicazioni software così chiamate negli smartphone e tablet
[110] Questa è una particolarità che si verifica con certe configurazioni di rete in ambito aziendale. I telefoni Blackberry hanno avuto un forte calo nel mercato. Resistono solo nel mercato aziendale. Noto per essere utilizzato dal presidente USA con delle applicazioni di sicurezza aggiuntive però del tutto particolari naturalmente.

.....3.3.- Il problema dell'accesso mediante impronte digitali

La sicurezza è un tema che porta spesso a grandi cambiamenti nell'informatica. La necessità di rendere sicure le informazioni più sensibili crea la necessità di sistemi di accesso sempre più difficili da eludere e di facile utilizzo per gli utenti. Una di queste nuove prospettive di recente forma è l'autenticazione biometrica. Portare le credenziali di accesso a livello personale ci permetterà di utilizzare nostre parti (del corpo) per prevenire accessi indesiderati da parte di malintenzionati.

Quanto premesso è chiaramente già in parte utilizzato dalle aziende e in particolare da quelle produttrici di dispositivi mobili (per esempio Apple e Samsung).

L'impronta digitale è una di queste. Ci caratterizza, le abbiamo praticamente tutti, e non è facile da clonare.

Non è facile ma non è impossibile[111]. La fotocamera posteriore scannerizza l'impronta ma è pur sempre una foto.

Comunque oggi esiste la possibilità per alcuni dispositivi di accedere con l'impronta digitale anziché con la *password* (anche se poi viene richiesto comunque l'inserimento di una password per eventuali sblocchi) e questo potrebbe porre altri problemi come sta avendo negli Stati Uniti[112]. Qui il giudice ha stabilito che il Quinto Emendamento copre soltanto le password personali, e non le impronte digitali. Questo significa che i poliziotti possono legalmente costringere il sospettato a sbloccare l'iPhone tramite Touch ID, e questa sentenza, negli USA, cambia le modalità di accesso ai codici personali. Le impronte digitali, non rientrano in questa casistica in quanto vengono equiparate ad un campione di DNA o ad una chiave fisica: in pratica, il cittadino è costretto ad "aprire" il proprio *smartphone* tramite impronta digitale.

Questo fatto naturalmente pone dei problemi perché assicura meno tutele al cittadino.

Tra l'altro inoltre la tradizionale SIM sparirà con altre tipi di conseguenze[113].

Comunque per accedere allo *smartphone* esistono metodi alternativi da remoto e quindi le cose acquistano ancora maggiore complessità.

Argomenti giuridici e nuovi sono quindi la non collaborazione ad apporre la propria impronta e nel caso di morte del proprietario ci si chiede il comportamento da adottare.

---

[111] http://www.repubblica.it/tecnologia/2014/12/30/news/sicurezza_le_impronte_digitali_non_saranno_il_futuro_basta_una_foto_per_clonarle_test_sul_ministro_della_difesa_tedesco-104006218/

[112] http://www.iphoneitalia.com/usa-la-polizia-puo-costringerti-a-sbloccare-liphone-usando-il-touch-id-ma-non-la-password-555222.html

[113] http://www.wired.it/mobile/smartphone/2015/07/17/cellulari-no-sim/

Naturalmente vincoli giuridici a parte ogni dispositivo elettronico mobile è attivabile e le sue protezioni sono aggirabili in *primis* con la collaborazione del produttore[114] che, solitamente pone ai dispositivi cosiddette *backdoor*[115] che aggirano gli ostacoli.

Nel nostro paese dove vige una legislazione diversa probabilmente qualora non si dovesse avere collaborazione da parte del soggetto si potrebbe ricorrere all'incidente probatorio.

.-4 Conclusione

Non si poteva giungere alla *mobile forensics* senza affrontare prima la *digital forensics*. Non lo si poteva fare perché molti dei principi procedurali giuridici e tecnici affrontati in essa restano a fondamento delle analisi forensi sviluppate negli apparati mobili.

Detto questo però si è da subito compreso, entrando maggiormente nei dettagli tecnici dei terminali mobili, che hanno caratteristiche tali da distinguerli dai tradizionali computer e che pertanto richiedono trattamenti particolari.

La *mobile forensics* rivolta alla telefonia mobile, oggi identificata sostanzialmente con gli *smartphone*, è una disciplina che presenta diverse complicazioni.

Il perché lo si è incardinato quasi da subito con il fatto che sono terminali sempre connessi alla rete mobile con la quale dialogano costantemente per il solo fatto del mutuo riconoscimento con le celle di zona.

Sono caratterizzati inoltre da una portabilità notevole date le loro ridotte dimensioni e auto alimentazione.

Queste caratteristiche si è constatato li rendono instabili nel senso che il loro stato varia continuamente.

Ecco perché una delle prime cose da farsi prima di procedere alla sua analisi è quella di isolarlo dal resto del mondo esterno.

Non basta però perché si è anche visto che se pur nella stragrande maggioranza dei casi sono supportati da uno stesso *vendor* e quindi modellati con uno stesso sistema operativo, in alcune situazioni sono adottate soluzioni proprietarie che rappresentano una complicanza in più nell'analisi.

---

[114] http://www.tomshw.it/news/l-iphone-e-nudo-ios-e-pieno-di-backdoor-messe-da-apple-59817
http://www.sciencedirect.com/science/article/pii/S1742287614000036

[115] "Porte di servizio" informatiche che aggirano le protezioni di sicurezza di un dispositivo

Con tali premesse e argomentazioni si è posto poi l'accento sugli accertamenti tecnici ripetibili o non ripetibili relativamente a questi dispositivi mobili e si è riscontrata una propensione agli accertamenti tecnici non ripetibili.

L'operatore tecnico, lo si è sottolineato, dovrà porre la massima attenzione e informare subito l'autorità inquirente dopo aver ricevuto l'incarico di questi fatti in modo tale da non vanificare il lavoro che andrà a svolgere.

Oramai la telefonia mobile è interconnessa con la rete Internet attraverso la quale i *vendor* aggiornano il dispositivo e forniscono applicativi vari. In più possono gestire e far gestire da remoto il dispositivo.

A riguardo si pensi ad un sequestro di uno *smartphone* che a detta dell'autorità giudiziaria potrebbe contenere elementi sensibilissimi. Qualora questo non fosse disconnesso dalla rete immediatamente, nel senso più pieno del termine, il terminale potrebbe essere resettato o bloccato dal proprietario, o da altri soggetti a lui legati, da remoto con la conseguente perdita di tutti i dati.

A parte la volontarietà di questi atti sicuramente penalmente rilevanti, potrebbe anche succedere più banalmente che alcuni aggiornamenti di sistema aspettino un benestare, anche implicito con il riavvio, per essere installati, con la conseguenza di una modificazione dello stato.

Non va dimenticato inoltre il rapporto sempre più intenso con il *cloud* che apre nuove frontiere nell'analisi forense.

CONCLUSIONI

.-1 Introduzione

Già nelle parte introduttiva della dissertazione si è evidenziato come i dispositivi elettronici siano utilizzati con una frequenza sempre più crescente dall'uomo moderno nella sua attività lavorativa e non.

Si è inoltre sottolineato che per le loro caratteristiche costruttive questi dispositivi raccolgano, chi più chi meno, le informazioni concernenti la condotta dei loro possessori nelle loro memorie elettroniche o, alternativa emergente di questi tempi, in spazi esterni normalmente identificati come *cloud storage.*

Queste tracce informatiche possono quindi ritornare molto utili nella formazione della prova nel processo penale qualora si abbia a dover dimostrare l'accadimento di un determinato fatto imputabile ad un certo soggetto all'interno di uno spazio temporale definito.

Svariati possono essere gli esempi. Uno di questi potrebbe essere quello di aver usato un certo *social network* o di avere scritto una certa *e-mail* magari a quell'ora o più semplicemente di possedere immagini riconducibili a comportamenti vietati dalla legge o di essere stati in un certo luogo perché localizzati, nel caso di un *smartphone*, da un cella telefonica o dal gps[116] che ha memorizzato nei suoi log le coordinate.

L'attenzione in questo lavoro è stata rivolta ai *mobile device* ed in particolare ai cellulari ormai evoluti in *smartphone* certi che questi rientrano a pieno titolo, per quanto riguarda le indagini probatorie, nella categoria della *mobile forensics* tra l'altro confermata essere una sottocategoria della più ampia *digital forensics*.

Per descrivere più pienamente la *mobile forensics* e le problematiche connesse ad essa nel processo penale si è ritenuto essenziale sviluppare una esposizione che dopo avere illustrato, nei sui principi base, alcuni dei principali istituiti del processo penale passasse obbligatoriamente attraverso la *digital forensics* quale elemento prodromico della *mobile forensics*.

[116]Alcune applicazioni (app) geolocalizzano l'utente per default. Quindi nei *file* di log dell'applicazione ve ne sarà traccia.

.-2 Sintesi delle osservazioni

Nel primo capitolo si sono analizzati se pur in superficie, i principali istituti del processo penale.

Di particolare interesse sono stati i mezzi di ricerca della prova quali perquisizione, ispezione, e sequestro. In questi si è cercato di coglierne oltre ai caratteri essenziali, le modifiche e integrazioni intervenute con la ratifica della convenzione di Budapest recepita con la legge n. 48/2008.

Alcuni di questi istituti infatti pur conservando le loro fondamenta risentivano del tempo e della necessità di un adeguamento che doveva legarsi al progresso[117] tecnologico proprio in virtù delle emergenti indagini informatiche.

Da tempo se ne ravvisava la necessità, come peraltro più volte sottolineato dalla dottrina, di operare sui sistemi informatici secondo modalità e comportamenti adeguati dal punto di vista operativo.

Il legislatore si occupa finalmente, cominciando nel 2001 e finendo nel 2008, di confrontarsi sulle misure da adottarsi e dirette ad assicurare la conservazione dei dati digitali originali.

Dopo questa necessaria inquadratura storica, si è posta, come conseguenza logica l'attenzione su alcune delle problematiche, non residuali, correlate alla acquisizione delle prove informatiche (*digital evidence*) che devono avvenire senza alterare l'originalità della prova. La clonazione, quel processo di esatta replicazione della prova digitale, non è equiparabile a una semplice acquisizione di copia del documento (art. 258 c.p.p.) ed è suffragato anche dal fatto che l'art. 254 bis c.p.p. nel riferirsi ai dati presso fornitori di servizio si esprime in termini di sequestro.

Si è anche posta l'attenzione sulle particolarità delle prove informatiche e alla loro intrinseca fragilità perché connotate da immaterialità e alterabilità.

Si è fatto inoltre cenno alle problematiche relative alla sua salvaguardia e alla sua esecuzione, nota come *bitstream image*[118] dovendo avvenire in modalità bit a bit.

---

[117]Nel campo digitale e quindi anche elettronico può essere interessante per significare quantitativamente il progresso ricordare la cosi detta legge di More (Gordon More, 1965) con la quale intuì che "Le prestazioni dei processori e il numero di transistor ad essi relativi raddoppiano ogni 18 mesi". Nel bene e nel male la pseudo-legge non è ancora stata smentita.

[118] Si ribadisce che la copia forense *bitstream image* deve contenere anche lo spazio non allocato. E' un po' come fare la copia ad un documento cartaceo che riserva ancora delle parti non usate ma che chiaramente rientrano nella copia fotostatica.

A chiudere il "cerchio" sulla formazione della prova e della sua validità probatoria interviene la catena di custodia della prova che è un paradigma procedurale assolutamente necessario.

Si è ribadita subito dopo l'attenzione che si deve riservare alle leggi scientifiche e al loro uso nella conseguimento della prova.

L'argomento è di sicuro interesse in quanto l'informatica[119] è una scienza relativamente nuova se pur sia il prodotto di scienze già affermate. Al pari delle altre scienze è comunque materia soggetta a continue verifiche.

Stabiliti come già evidenziato nel primo capitolo i fondamenti del processo penale nella fase probatoria si è, con il secondo capitolo, introdotta la *digital forensics*.

Si è visto come i suoi contorni siano ancora non completamente definiti e in continua evoluzione. È essa stessa un incontro tra le scienze forensi e le scienze informatiche. Ecco perché il mondo giuridico ha necessità di interfacciarsi con il mondo tecnologico e viceversa in una condizione quindi di massima simmetria collaborativa possibile.

E' stato necessario delineare, con una certa generalità, le architetture dei dispositivi elettronici e compreso anche come sia possibile, quasi sempre, ricondurle ad una base fondamentale comune.

Non si poteva prescindere da queste argomentazioni tecniche se si voleva coglierne con più efficacia i risvolti giuridici nella fase di indagine probatoria.

La *digital forensics* ha anche a sua disposizione innumerevoli strumenti tecnici utili alle analisi dei sistemi informatici.

Nel descrivere questi *tool* si è cercato di comprenderne attraverso le loro funzionalità le problematiche ricorrenti alle quali spesso l'operatore (Polizia Giudiziaria o consulente tecnico che sia) incontra nella fase di acquisizione probatoria.

La *digital forensics* ha diversi sotto settori che ora , allo stato delle cose, si ritrovano principalmente[120] nella *computer forensics*, *network forensics*, *mobile forensics* e *cloud forensics* ma che probabilmente sono destinati ad ampliarsi anche perché ognuno di essi

---

[119] http://www.treccani.it/vocabolario/tag/informatica/ "Scienza che studia l'elaborazione delle informazioni e le sue applicazioni; più precisamente l'i. si occupa della rappresentazione, dell'organizzazione e del trattamento automatico della informazione. Il termine i. deriva dal fr. informatique (composto di INFORMATion e automatIQUE, «informazione automatica" così ancora più precisamente "dal fr. *Informatique*, comp. di i*nform(ation electronique ou autom)atique* anche dal vocabolario della lingua italiana Lo Zingarelli Edizione XXII

[120] Alcune nuove tendenze intravedono anche la video forensics, l'audio forensics, la chipp-off forensics e la OSINT forensics (accesso banche dati pubbliche). Un quadro quindi in forte espansione. Naturalmente con una richiesta di maggiore specializzazione

comporta nuove sfide rispetto ad un progresso tecnologico sostanzialmente instabile e mutevole. I settori sono tra di loro altamente in relazione.

Di notevole interesse poi, e di forte pertinenza, è stato poi il tema dell'accertamento ripetibile e irripetibile, talvolta non nettamente definito neanche dal legislatore, declinandolo per quanto possibile in particolare per i dispositivi mobili e quindi nella *mobile forensics*.

Con il terzo capitolo si è affrontato il tema centrale del presente lavoro costituito dalla la *mobile forensics* quale macro componente naturale della *digital forensics*. La logica conseguenza è che gran parte dei temi affrontati per essa valgono inevitabilmente per l'analisi dei *mobile device*.

Questi ultimi però si distinguono per alcune particolarità come quelle che che li legano all'utilizzo della rete mobile e anche per il fatto di essere facilmente trasportabili perché leggeri e auto alimentati.

Questi dispositivi hanno un rapporto di continuo scambio con la rete mobile (con le celle) il che pone lo stato del *device* in una situazione di perenne "instabilità".

Il *device* deve essere quindi, una volta posto sotto analisi allo scopo di cristallizzare una certa situazione, protetto da alterazioni, isolandolo dalla rete mobile. Ma in termini di paragoni non è equiparabile ad un distacco dalla rete di un computer. In questi casi infatti non basta, e lo si è argomentato, la semplice disconnessione del cavo di rete.

I *mobile device* sono oggetti che subiscono continue modifiche tecnologiche sia nel lato hardware che software e perciò sono spesso sistemi complessi da analizzare in modo certo.

Qui, si è osservato che la ripetibilità degli accertamenti è meno scontata che in altri dispositivi.

.-3 Valutazioni conclusive

La *digital forensics*, si è visto, è una disciplina o meglio, ad avviso di chi scrive, una scienza che abbraccia fattori di natura fortemente tecnici coniugata alle scienze giuridiche. La *digital forensics* è inoltre una materia che, pur avendo dei fondamenti solidi e per certi versi immutabili come le leggi dell'elettronica e dell'informatica, subisce profonde mutazioni legati al progresso tecnologico. Questa dinamica evolutiva dei mezzi e delle tecnologie digitali impone ogni giorno approcci differenti nell'affrontare le analisi informatiche ai fini forensi. L'impressione è che le norme giuridiche non sempre si adeguino a queste dinamiche. La colpa può ritrovarsi anche nella formazione delle disposizioni legislative. Un interessante prospettiva potrebbe essere quella di costruire una base normativa di principi generali, come nel caso della normativa della privacy, Decreto legislativo 30 giugno 2003, n. 196, al quale associare un allegato tecnico più facilmente mutabile a seconda degli sviluppi tecnici e con una gestione più propriamente tecnica.

Resta comunque la difficoltà tipica di quando si debbano sposare norme tecniche con norme giuridiche. Spesso il legislatore ha difficoltà a recepire i mutamenti tecnologici e tradurli in disposizioni normative e spesso l'autorità giudiziaria ha difficoltà nel comprendere pienamente tali nature tecniche.

Il problema tocca naturalmente anche le consulenze tecniche che spesso non appaiono adeguate in quanto l'autorità giudiziaria non ha, verso queste figure, elevate pretese. La legge non richiede specifiche conoscenze o requisiti particolari e la conseguenza e che spesso vengono forniti pareri superficiali o fuorvianti. Gli standard procedurali o protocolli o meglio ancora le *best practices* sono per lo più di derivazione straniera.

Di interesse a riguardo è quanto prevede, per esempio, l'associazione IACIS[121] che unisce un codice etico a delle specifiche conoscenze i cui associati devono possedere[122] e che qui per ovvie ragioni si sintetizzano:

- mantenere il più alto livello di oggettività in tutte le procedure di esame forense e presentare con precisione e cura tutti i fatti coinvolti
- esaminare in modo preciso e con grande cura la prova
- condurre esami basati su principi stabiliti e validi
- fornire delle opinioni che abbiano una base ragionevolmente dimostrabile

[121] http://www.iacis.com/ The International Association of Computer Investigative Specialists e http://www.iacis.com/SiteAssets/Documents/IACIS%20Certification%20Policy%20v3.0.pdf

[122] Qui si è naturalmente voluto sintetizzare.

– non si devono fornire informazioni ingannevoli con riferimento alle proprie credenziali, alla propria istruzione, ai percorsi di training seguiti o al proprio stato di membro IACIS

- conoscere la normativa civilistica, penalistica, giuslavoristica con riferimento alla prova

- conoscere la disciplina penalistica dei reati informatici più comuni

Bisogna riconoscere che le nuove frontiere della *digital forensics* sono costantemente in espansione e che i sotto settori sono sempre più in relazione tra di loro. Oramai ogni dispositivo mobile è interconnesso con la rete Internet dove può allocare i propri dati in nuovi spazi virtuali che non hanno una ben definita collocazione fisica. Questa nuova frontiera è chiaramente quella del *cloud*.

Ecco perché molto probabilmente ci sarà bisogno anche di nuove forme di collaborazione tra Stati che dovranno tra loro cooperare.

I fornitori di questi servizi hanno sedi dislocate in tutto il mondo e quindi indagare oggi e ancora di più domani aprirà scenari inediti nuovi.

La trasportabilità dei sistemi informatici attraverso la costruzione di macchine virtuali attraverso i servizi di *cloud computing* con tariffazione a consumo che i vari *vendor* offrono, pone dal punto di vista della ricerca delle prove processuali, sempre nuove problematiche e sfide delle quali il legislatore non può non tener conto.

Un soggetto infatti potrebbe acquistare una macchina virtuale da un *provider* dello Stato A il cui server fisico è situato nello Stato B ma che viene replicato nello Stato C. Naturalmente la macchina virtuale potrà essere usata in ogni parte del mondo e si potrà accedervi con *smartphone*, *tablet*, *computer*.

Sarà sempre meno evidente la distinzione che esiste all'interno tra i vari settori della *digital forensics* e questo probabilmente rivoluzionerà anche la tecnica delle analisi forensi.

RIFERIMENTI

.-1 Normativa

.....1.1.- Documenti dell'Unione Europea e del Consiglio d'Europa

DIRETTIVA 2013/40/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 12 agosto 2013 relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio - L 218/8 Gazzetta ufficiale dell'Unione europea 14.8.2013

Rec(95)13E 11 September 1995 concerning problems of criminal procedural law connected with information technology

COUNCIL OF EUROPE COMMITTEE OF MINISTERS RECOMMENDATION No. R (95) 13 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES CONCERNING PROBLEMS OF CRIMINAL PROCEDURAL LAW CONNECTED WITH INFORMATION TECHNOLOGY (Adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies)

.....1.2.- Costituzione e Leggi ordinarie

Costituzione della Repubblica Italiana, art. 111

Legge 18 marzo 2008 n. 48: «Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno» Gazzetta Ufficiale n. 80 del 4 aprile 2008 - Supplemento Ordinario n. 79

DECRETO LEGISLATIVO 7 marzo 2005, n. 82 Codice dell'amministrazione digitale, pubblicato nella Gazzetta Ufficiale n.112 del 16-5-2005 - Suppl. Ordinario n. 93

.....1.3.- Codice di Procedura Penale

artt. 187, 189, 190, 192, 211,, 213, 215, 216, 218, 220, 221, 222, 223, 224, 225, 226, 233, 234, 244, 247,253, 254, 254-bis, 258, 259, 260, 316, 321, 348, 354, 359, 360, 392, 415 bis, 433, 510, 511

.-2 Giurisprudenza

Tribunale Penale monocratico di Bologna I sezione Sentenza n. 1823/2005 (cosi detto caso Vierika)

Corte di Cassazione - Sezione II penale - Sentenza 12 dicembre 2008-13 marzo 2009 n. 11135

Corte Di Assise Di Appello Di Milano Sezione II, 6.12.2011, n. 49/2010 Reg, p.14 (cosi detta sentenza Stasi)

Corte di Cassazione, sezione III penale,16.01.2014, n. 10491

.-3 Dottrina

AA. VV., Enciclopedia Tematica Le Garzantine, *Scienze*, Garzanti Libri, Milano, 2006

ALMA, M.M. *L'ingresso della prova scientifica nel processo penale (quesiti, tipi di accertamenti, rapporti con periti e consulenti ecc.) con particolare riguardo all'evoluzione nel tempo ed alla fallibilità della scienza in rapporto alla decisione da adottarsi «al di là di ogni ragionevole dubbio,* Consiglio Superiore della Magistratura commissione per la formazione della Magistratura Onoraria Distretto della Corte d'Appello di Milano, Milano, 9 febbraio 2010.

BASSETTI, M., *Indagini digitali vademecum di uno Sherlock Holmes informatico, 2011*

CLARKE, N., *Computer forensics,* UK, IT Governance Publishing

D'AIUTO G., LEVITA L., *I reati informatici disciplina sostanziale e questioni processuali,* Milano, 2012

DANIELE, M., *La prova digitale nel processo penale,* Rivista di Diritto Processuale CEDAM 2011 pp. 283-298

DI PAOLO, G., *Prova informatica (diritto processuale penale)*, Enciclopedia del Diritto, pp.736-762

DOMINIONI, O., *Prova scientifica (diritto processuale penale)*, in Enciclopedia del Diritto, pp. 976-998

DURANTE, M., PAGALLO, U., *Manuale di informatica giuridica e diritto delle tecnologie,* Torino, 2012

FERGUSON; N., SCHNEIDER; B., KOHNO, T., *Il manuale della crittografia : applicazioni pratiche dei protocolli crittografici*, Milano, Apogeo, 2011.

GIRARDINI, A. FAGGIOLI,G., *Digital Forensics,* Milano, 2013

RESTON, J., *Galileo*, Casale Monferrato (AL), 2001

TANEBAUM, A., *Architettura del computer. Un approccio strutturato*, MILANO, 2000

TONINI, P., *Considerazioni su diritto di difesa e prova scientifica,* 2013, http://www.archiviopenale.it/apw/wp-content/uploads/2013/06/il_punto_su_Tonini.pdf
TONINI, P., *Manuale di procedura penale,* 11 ed., Milano, 2010
UBERTIS, G., *Sistema di procedura panale I,* Torino, 2012
ZICCARDI, G., LUPARIA L*., Investigazione penale e tecnologia informatica,* Milano, 2007

.-4 Siti web

http://www.iacis.com/IACIS International Association of Colloid and Interface Scientists
http://leg15.camera.it/_dati/leg15/lavori/schedela/trovaschedacamera_wai.asp?PDL=2807
http://www.ibm.com/cloud-computing/it/it/what-is-cloud-computing.html X-Way Forensic -
http://csrc.nist.gov/publications/PubsSPs.html#800-101
http://www.nist.gov/ National Institute of Standards and Technology
http://lang.cellebrite.com/it/mobile-forensics/products/standalone/ufed-touch-ultimate
http://www.logicube.com/knowledge/celldek-tek - https://www.msab.com/
http://www.ibm.com/cloud-computing/it/it/what-is-cloud-computing.html
http://www.treccani.it/vocabolario/tag/informatica/
http://www.iacis.com/ The International Association of Computer Investigative Specialists
https://www.docenti.unina.it/downloadPub.do?tipoFile=md&id [La prova digitale]
http://www.procura.milano.giustizia.it/reati-informatici.html
http://lang.cellebrite.com/it/mobile-forensics/products/standalone/ufed-touch-ultimate
https://www.msab.com/
http://www.logicube.com/knowledge/celldek-tek
http://www.iacis.com/SiteAssets/Documents/IACIS%20Certification%20Policy%20v3.0.pdf
http://attivissimo.blogspot.it/2014/04/samsung-galaxy-s5-gia-scavalcato-il.html
http://www.hwupgrade.it/news/apple/iphone-5-inviolabile-contiene-segreto-di-un-omicidio-ma-apple-si-rifiuta-di-collaborare_50877.html
http://www.iphoneitalia.com/usa-la-polizia-puo-costringerti-a-sbloccare-liphone-usando-il-touch-id-ma-non-la-password-555222.html
http://www.onorarimilano.it/documentazione/D_476.doc
http://gnosis.aisi.gov.it/sito%5CRivista8.nsf/servnavig/14