

Il diritto processuale penale dell'informatica e le investigazioni informatiche*

Sommario

1 La computer forensics. - **2** Le origini della computer forensics. - **3** La prova digitale. - **4** Il documento informatico e il processo civile. - **5** Gli strumenti di ricerca della prova digitale nel processo penale. - **6** La ricerca e l'analisi del dato informatico. Una questione di metodo.

1 La computer forensics

Come non si è mancato di accennare nei precedenti capitoli, con particolare riferimento alla Ratifica della Convenzione di Budapest del 2001, il Legislatore Italiano ha preso atto dell'evoluzione tecnologica in corso ed ha quindi predisposto gli opportuni interventi legislativi necessari al fine di contrastare il sempre crescente fenomeno della criminalità informatica.

Allo stesso tempo, il Legislatore ha previsto adeguati strumenti d'indagine e nuove garanzie processuali con particolare riferimento alle investigazioni informatiche.

La costante presenza di apparecchiature informatiche e digitali sulla scena di un crimine, l'importanza delle informazioni in esse contenute, la fragilità e volatilità del dato informatico, l'importanza della corretta acquisizione e gestione delle prove informatiche, anche per il loro uso in dibattimento, sono condizioni che hanno creato il terreno fertile per la nascita di una nuova branca delle scienze forensi, nota come computer forensics (1).

* Capitolo a cura di A. LAZARI, Avvocato del Foro di Lecce, si occupa di Diritto dell'informatica e delle nuove tecnologie. È dottorando di ricerca presso il dipartimento di sistemi e informatica dell'Università degli studi di Firenze ed è cultore della materia in Informatica giuridica.

(1) ZICCARDI e LUPÀRIA sostengono che «contestualmente al mutuoamento portato, nelle società, dalle nuove tecnologie e, in particolare, dall'avvento dell'elaboratore elettronico e delle reti, si è verificato

Secondo la migliore dottrina, la computer forensics è «la disciplina che si occupa della preservazione, dell'identificazione, dello studio, delle informazioni contenute nei computer, o nei sistemi informativi in generale, al fine di evidenziare l'esistenza di prove utili allo svolgimento dell'attività investigativa» (2).

Ogni dispositivo tecnologico rinvenuto sulla scena di un crimine ha due distinti aspetti: quello fisico, ove si possono rinvenire impronte digitali e altri elementi di prova tipici degli oggetti di uso comune, e quello logico, costituito dai dati contenuti nella memoria del dispositivo.

L'esperto di computer forensics che si occupa di identificare, analizzare e produrre in giudizio delle prove informatiche, pertanto, deve possedere una specifica competenza ed esperienza in ambito informatico e telematico ed anche una buona conoscenza delle norme processuali attinenti principalmente le fasi di perquisizione, ispezione e sequestro. Non è raro che approcci sbagliati nella fase di acquisizione o gestione dei supporti informatici portino all'invalidazione della prova in essi rinvenuta, in sede di dibattimento.

2 Le origini della computer forensics

La genesi della computer forensics risale agli anni novanta, periodo in cui avvenne la diffusione dei primi personal computer, ed è collegata alle ricerche accademiche ed ai primi approcci effettuati dalle agenzie governative statunitensi.

Il processo di digitalizzazione delle informazioni relative alla vita personale e lavorativa di ogni individuo pose le basi per la nascita di questa disciplina che aveva come scopo principale quello di identificare, acquisire, analizzare e catalogare i dati presenti nei dispositivi elettronici per il loro uso in giudizio.

L'interpretazione del dato acquisito, infatti, diviene l'aspetto principale della computer forensics che si pone l'obiettivo di ricostruire gli eventi di un crimine attraverso l'analisi di un sistema informatico e dei supporti di memoria in esso contenuti.

La computer forensics, attraverso la sua sempre più frequente applicazione nel campo delle investigazioni informatiche e grazie anche alla

un cambiamento nelle modalità di rilevazione, gestione, raccolta ed analisi di elementi che, in senso lato e assolutamente generico, si potrebbero definire fonti di prova, prova, indizio o testimonianza» in LUPARIA-ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2008, 3 e ss.

(2) GHIRARDINI-FAGGIOLI, *Computer Forensics*, Milano, 2009, 1 e ss., LUPARIA, ZICCARDI, op. cit., 3 e ss.

maggiore specializzazione acquisita dai corpi di polizia e dai consulenti tecnici, ha assunto nuove denominazioni a seconda dello specifico campo di applicazione.

Alla computer forensics, infatti, sono state affiancate ulteriori discipline affini, quale la network forensics, cui scopo principale è l'acquisizione del dato in transito su una rete telematica (cd. intercettazione di dati o comunicazioni) e la *mobile forensics* che si occupa dell'analisi dei telefoni cellulari e dispositivi palmari.

Tale suddivisione in categorie non sempre risulta essere esaustiva poiché l'evoluzione tecnologica e la convergenza dei servizi offerti dai dispositivi elettronici rende sempre più difficile la loro specifica catalogazione in una determinata categoria, e, talvolta, rende ancor più difficile l'operazione di acquisizione del dato in essi contenuto soprattutto in mancanza di adeguata documentazione che consenta al tecnico di comprendere perfettamente le caratteristiche tecniche ed operative del dispositivo sottoposto ad indagine (3).

La diffusione delle tecnologie ha, quindi, ampliato notevolmente il campo di indagine delle autorità e dei tecnici del settore, i quali si sono trovati di fronte ad uno scenario composto da molteplici sfaccettature e caratterizzato dalla sempre crescente presenza di informazioni utili alle indagini, contenute, non solo nei computer, ma anche in dispositivi quali, ad esempio, consolle portatili, lettori digitali ed anche navigatori satellitari.

Lo studio e l'applicazione di nuove tecniche di computer forensics ha avuto ulteriore impulso a seguito degli attentati terroristici avvenuti nel settembre 2001 negli Stati Uniti.

La sempre crescente centralità delle tecnologie nell'organizzazione di attentati, nonché il sempre più frequente uso di Internet per la comunicazione tra cellule terroristiche e per gli attacchi a infrastrutture critiche, ha spinto i governi a porre in essere nuove misure volte alla lotta e prevenzione del terrorismo telematico, o cyber terrorismo.

Questo fenomeno ha portato le forze di polizia e le agenzie governative a gestire una enorme quantità di dati generata dalle intercettazioni telematiche effettuate sulla rete Internet.

Il sensibile aumento delle intercettazioni telematiche e la facilità di intercettazione di dati su sistemi privi di adeguate misure di sicurezza ha dato

(3) Si pensi all'acquisizione di dati da dispositivi destinati a mercati differenti da quello Italiano e con i quali il perito può non avere dimestichezza. Ogni tentativo di effettuare un'acquisizione su un dispositivo di cui non si conosce l'esatto funzionamento può portare all'alterazione o distruzione della prova. Una situazione del genere si verificava in Italia, nel 2001, con l'arrivo dei primi modelli di iPod. La stessa situazione si è riproposta nel 2007 con la commercializzazione dei telefoni cellulari chiamati iPhone che dispongono di un particolare blocco, integrato nel sistema operativo, che impedisce l'accesso alla memoria del dispositivo.

vita ad un fenomeno di contrasto della computer forensics, noto come anti-forensics.

L'anti-forensics studia l'uso delle tecnologie al fine di impedire le indagini ed i controlli effettuati con procedure di computer forensics.

Tale nuova disciplina è figlia di due differenti necessità, quella del tutto lecita che mira a proteggere il dato informatico da accessi non autorizzati anche al fine di garantire la riservatezza dei dati personali e quella che ha come scopo quello di impedire l'esecuzione di indagini informatiche mediante la cancellazione delle tracce relative ad un'attività delittuosa, ovvero mediante il vero e proprio sviamento delle indagini mediante l'attività di depistaggio informatico.

3 La prova digitale

Nasce, quindi, il concetto di «prova digitale» caratterizzata dalle qualità proprie del dato informatico, ovvero l'immaterialità e la fragilità. Per la sua corretta acquisizione vengono sviluppati una serie di strumenti, hardware e software, che vanno utilizzati in tutto il procedimento di acquisizione, analisi e conservazione della prova digitale ed anche ai fini della verificabilità delle procedure e dei metodi utilizzati dal perito nell'indagine.

Obiettivo della computer forensics, ai fini della piena validità della prova e della sua utilizzabilità in giudizio, è la verificabilità delle procedure attuate durante l'intera indagine informatica. La trasparenza delle operazioni compiute e la loro ripetibilità innanzi al magistrato giudicante, sono *condicio sine qua non* di ogni perizia in materia di investigazioni informatiche.

L'accennata fragilità del dato, contenuto nelle memorie rinvenute all'interno dei più disparati dispositivi, impone all'investigatore informatico l'uso di particolari cautele nella gestione delle fonti di prova, nonché l'obbligo di procedere sempre, in via preliminare, all'esecuzione di un duplicato o «bit to bit», del supporto di memoria oggetto di indagine.

Secondo Ziccardi, il valore probatorio della prova informatica è inteso come «capacità di resistenza ad eventuali contestazioni e capacità di convincimento del giudice, delle parti processuali o di altri soggetti in ordine alla genuinità, non ripudiabilità, imputabilità e integrità del dato stesso e dei fatti dallo stesso dimostrati» (4).

(4) LUPARIA-ZICCARDI, op. cit., 11 e ss.

4 Il documento informatico e il processo civile

Nel procedimento civile, la prova serve all'attore per dimostrare i fatti costitutivi della pretesa vantata in giudizio ed a convincere il magistrato della fondatezza delle proprie richieste.

In tale sede assumono particolare rilevanza, a livello probatorio, le prove precostituite, cioè quelle prove formate al di fuori del processo e che vengono prodotte in giudizio dalle parti.

Le più importanti prove precostituite sono quelle documentali, ovvero l'atto pubblico, la scrittura privata e la riproduzione meccanografica.

Tra le prove documentali rientra anche il documento informatico, la cui idoneità a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità (5). Identico valore probatorio è previsto anche per il documento informatico sottoscritto con firma elettronica (6).

Il documento informatico sottoscritto con firma digitale o altra firma elettronica qualificata (7), invece, ha valore di prova legale ed assume l'efficacia prevista dall'art. 2702 c.c. (8).

Un qualsiasi documento informatico sottoscritto con firma digitale o altra firma elettronica qualificata, prodotto in un giudizio civile avrà, quindi, lo stesso valore probatorio previsto per la scrittura privata, salvo che il titolare del dispositivo di firma non proponga querela di falso, fornendo la prova che la sottoscrizione è avvenuta contro la sua volontà.

(5) Art. 20 co. 1 bis del Codice dell'amministrazione Digitale «L'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dal comma 2».

(6) Art. 21 co. 1 del Codice dell'amministrazione Digitale «Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità».

(7) Art. 21 co. 2 del Codice dell'amministrazione Digitale «Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria».

(8) Art. 2702 c.c. - *Efficacia della scrittura privata* «La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta».

5 Gli strumenti di ricerca della prova digitale nel processo penale

Nel giudizio penale, la prova aiuta il magistrato a valutare se la condotta dell'imputato integri una fattispecie di reato prevista dalla legge.

Passando all'analisi della prova all'interno del processo penale, quindi, occorre preliminarmente evidenziare che la stessa si forma in contraddittorio tra le parti coinvolte nel giudizio, durante il dibattimento.

Nel processo penale, inoltre, il giudice può disporre l'acquisizione di qualunque mezzo di prova ritenuto idoneo all'accertamento dei fatti purché non pregiudichino la libertà morale della persona (9).

Al contrario delle rigide disposizioni che regolano il processo civile, nel processo penale le prove non sono previste tassativamente in quanto il magistrato giudicante può ammettere qualunque prova, anche se non prevista dalla legge, purché sia idonea a ricostruire i fatti.

Anche nel processo penale è ammessa l'acquisizione di prove documentali, tra le quali rientra anche il documento informatico, per come descritto nel paragrafo precedente.

Il processo penale, al contrario di quello civile, non è caratterizzato dalla tipicità dei mezzi di prova ammissibili, ma dagli strumenti previsti dal legislatore per la ricerca di fonti di prova a sostegno dell'accusa.

La ricerca dei mezzi di prova ricade principalmente all'interno della delicata fase delle «indagini preliminari», imperniata sull'attività investigativa svolta dall'autorità giudiziaria, sotto la direzione ed il costante controllo del pubblico ministero e volta ad acquisire elementi di prova che consentano di ricostruire gli eventi ed a sostenere, se del caso, l'accusa.

I mezzi di ricerca della prova previsti dal codice di procedura penale sono le ispezioni, le perquisizioni, i sequestri e le intercettazioni.

Le ispezioni, disciplinate dall'art. 244 c.p.p. (10), sono disposte con decreto motivato del pubblico ministero «quando occorre accertare le tracce e gli altri effetti materiali del reato».

(9) Art. 189 c.p.p. «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».

(10) Art. 244 c.p.p. «L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato».

2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica [...].»

Il Legislatore è intervenuto (11) sull'articolo dedicato alle ispezioni con l'aggiunta di un periodo alla fine del secondo comma: «anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione». La norma, quindi, introduce il concetto di «misure tecniche» volte all'acquisizione e conservazione del dato originale, nonché misure per la sua conservazione, elementi mutuati dalle nozioni di base della computer forensics.

Il trattamento del dato nelle fasi di ispezione, perquisizione o sequestro, è il momento più delicato della fase investigativa, poiché è proprio durante la fase di primo accesso al dato che l'operatore, in caso di mancata applicazione di un corretto metodo di lavoro, rischia di compromettere seriamente l'indagine mediante l'alterazione, cancellazione o sovrascrittura di un dato rilevante per l'impianto accusatorio.

L'evoluzione dell'informatica e lo sviluppo di sempre nuove e diverse apparecchiature in grado di immagazzinare dati, ha aperto nuove problematiche connesse all'esercizio delle attività di ispezione a causa delle notevoli difficoltà che si incontrano nella ricerca del dato informatico (12).

Le difficoltà, inoltre, non sono limitate alla sola ricerca del dato, ma anche all'accesso allo stesso, vista la sempre crescente adozione di sistemi software e hardware che consentono di nascondere dati all'interno di aree di memoria nascoste o cifrate.

Il legislatore è intervenuto, con aggiunte, anche in tema di perquisizioni (13) prevedendo la possibilità di estendere tale strumento di ricerca della prova anche ai sistemi informatici. Tale attività, al pari di quella ispettiva,

(11) Art. 8 legge 48/2008 "Modifiche al titolo III del libro terzo del codice di procedura penale".

(12) La ricerca della prova digitale, nelle ispezioni, non si deve limitare ai soli sistemi informatici tradizionali, quali computers o laptop, ma deve essere estesa a qualsiasi dispositivo capace di contenere informazioni digitali. Si pensi ai lettori multimediali, alle fotocamere digitali, alle pen drive usb ed anche ai navigatori satellitari dotati di memorie esterne per la memorizzazione delle mappe.

(13) Art. 247 c.p.p. «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 vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.

1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando le misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

2. La perquisizione è disposta con decreto motivato.

3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto». Questo articolo è stato modificato dall'art. 8 della legge 48/2008 mediante l'aggiunta del comma 1-bis.

necessità di personale specializzato che sia adeguatamente addestrato anche nel «decision making», vista la delicatezza del dato e le possibili ripercussioni in caso di sua accidentale alterazione o cancellazione.

Anche in tema di sequestro (14), l'informatica ha posto nuove problematiche agli operatori di diritto ed alle autorità che eseguono il decreto che dispone il sequestro.

Normalmente, infatti, il sequestro di apparecchiature informatiche si limita alle sole memorie contenute all'interno del sistema oggetto di indagine. In dottrina si discute addirittura della possibilità di evitare l'interruzione del funzionamento del sistema informatico oggetto di indagine attraverso l'esecuzione della sola copia originale dei supporti di memoria.

Questo accade nei casi in cui l'attività di indagine è limitata alla sola acquisizione di dati, ovvero quando l'attività di indagine si ferma al solo aspetto «logico» ed immateriale del sistema informatico.

Nel caso in cui, invece, l'attività debba essere estesa al componente «fisica» del sistema, per la ricerca, a titolo di mero esempio, di impronte digitali o elementi simili, l'autorità provvederà all'imballaggio e sequestro delle periferiche quali tastiera, mouse, schermo ed altre strumentazioni o apparecchiature «pertinenti».

Il Legislatore con le modifiche al codice di procedura penale introdotte con la legge 48/08 ha, altresì, formulato una nuova norma inerente il sequestro di dati informatici presso fornitori di servizi informatici e telematici e di telecomunicazioni (15) con espressa previsione dell'obbligo di adozione di opportune misure volte alla tutela dell'integrità del dato acquisito ed alla sua conformità al dato originale.

La stessa norma prevede la concreta possibilità di ordinare al service provider di «conservare e proteggere adeguatamente i dati originali» con obbligo, quindi, di evitare che gli stessi vengano alterati o distrutti.

(14) Art. 253 c.p.p. «1. L'autorità giudiziaria dispone con decreto motivato 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 ovvero un ufficiale di polizia giudiziaria delegato con lo stesso decreto.

4. Copia del decreto di sequestro è consegnata all'interessato, se presente».

(15) Art. 254 - bis c.p.p. «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 non modificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali».

Ulteriore e non meno importante strumento di indagine è quello costituito dalle intercettazioni di conversazioni e comunicazioni (16) che rientra per lo più nella disciplina denominata network forensics.

Le attività di intercettazione, al pari degli altri strumenti di ricerca delle fonti di prova, hanno dovuto affrontare le problematiche poste dalle comunicazioni mediante reti telematiche ed alle difficoltà tecniche legate alla loro intercettazione.

Scopo delle intercettazioni è quello di captare in tempo reale il flusso di dati che attraversa una rete telematica e rendere il loro contenuto intelligibile in sede di dibattimento.

Questo tipo di attività di indagine non costituiva un problema nel momento in cui gli operatori di polizia dovevano affrontare intercettazioni di comunicazioni su rete fissa o mobile.

Da qualche tempo, però, soprattutto negli ambienti della criminalità informatica e del terrorismo, gli «obsoleti» strumenti di comunicazione, inclusi i messaggi di posta elettronica, sono stati abbandonati a scapito di tecnologie di tipo «voice over internet protocol»(voIP) (17) che consentono comunicazioni molto sicure e che sono di difficile intercettazione poiché utilizzano avanzati algoritmi di crittografia che, in taluni casi, sono molto difficili o impossibili da decifrare.

Un caso emblematico è quello costituito dal software denominato Skype (18) che consente di effettuare chiamate di tipo video e audio mediante l'uso della tecnologia «voip». Lo stesso consente anche di scambiare messaggi immediati (di tipo chat) e files di ogni genere.

La caratteristica che ha reso Skype il software usato da oltre 400 milioni di utenti nel mondo è costituita dall'impossibilità di intercettare i contenuti delle conversazioni poiché la società produttrice del software ha applicato al programma, a più livelli, una serie di algoritmi di cifratura proprietari.

(16) Art. 266 c.p.p. «1. L'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione è consentita nei procedimenti relativi ai seguenti reati:

- a) delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni determinata a norma dell'art. 4;
- b) delitti contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni determinata a norma dell'art. 4;
- c) delitti concernenti sostanze stupefacenti o psicotrope;
- d) delitti concernenti le armi e le sostanze esplosive;
- e) delitti di contrabbando;
- f) reati di ingiuria, minaccia, molestia o disturbo alle persone col mezzo del telefono.

2. Negli stessi casi è consentita l'intercettazione di comunicazioni tra presenti. Tuttavia, qualora queste avvengano nei luoghi indicati dall'art. 614 c.p., l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa».

(17) Il Voice Over Internet Protocol è una tecnologia che consente di comunicare attraverso l'uso delle reti telematiche.

(18) www.skype.com

L'impossibilità di intercettare le comunicazioni effettuate mediante l'uso del software Skype ha portato il Ministero dell'Interno a costituire un pool di esperti con lo scopo specifico di tentare di comprendere i meccanismi del suo funzionamento e rendere possibile la sua intercettazione (19).

L'uso di Skype ha spinto le forze di polizia a ripiegare su «vecchi» metodi di intercettazione, quali le intercettazioni ambientali, che consentono, però, di captare una sola parte della conversazione, soprattutto se uno dei due utenti si trova al di fuori dei confini nazionali.

6 La ricerca e l'analisi del dato informatico. Una questione di metodo

Una volta esaurite le fasi di ricerca delle fonti di prova, i supporti sequestrati devono essere sottoposti ad approfondite analisi al fine di recuperare le informazioni in essi contenute.

Questo tipo di attività, in mancanza di un reparto di polizia specializzato, è solitamente demandata ad un consulente tecnico incaricato mediante lo strumento dell'accertamento (20) che costituisce ulteriore sfaccettatura delle attività di indagine disposte dal pubblico ministero.

L'analisi dei reperti informatici è solitamente influenzata da due variabili principali, quella tecnologica, legata alle caratteristiche della strumentazione oggetto di indagine, circostanza che richiede l'uso di numerose e costose attrezzature, e quella soggettiva, legata all'esperienza del tecnico che si occupa di effettuare le indagini.

L'uso di tecnologie non adeguate o appartenenti a standard non conformi, aggiunte all'uso di «infelici» tecniche di analisi dei supporti, possono seriamente compromettere l'esito di un giudizio.

È per questo motivo che la prassi investigativa ha elaborato una serie di linee guida investigative, dette «best practice» (21), che sono general-

(19) www.interno.it/mininterno/export/sites/default/it/sezioni/sala_stamp/comunicati/comunicati_2009/0895_2009_02_18_skype.html_2100293813.html. «Il ministro dell'Interno, Roberto Maroni, ha costituito un apposito Gruppo di lavoro formato da rappresentanti del Dipartimento della Pubblica Sicurezza, dalla Polizia di Stato, Carabinieri, Guardia di Finanza e dal Consiglio Nazionale delle Ricerche, che ha l'obiettivo di ricercare soluzioni tecnologiche e normative per rendere fruibili ai fini investigativi e giudiziari le intercettazioni telematiche effettuate sulle conversazioni Voip che utilizzano il software prodotto da Skype».

(20) Art. 359 c.p.p. «1. Il pubblico ministero, quando procede ad accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze, può nominare e avvalersi di consulenti, che non possono rifiutare la loro opera.

2. Il consulente può essere autorizzato dal pubblico ministero ad assistere a singoli atti di indagine».

(21) Il termine «best practices» è mutuato dalle esperienze scientifiche statunitensi che costituiscono il punto di riferimento principale nel settore delle investigazioni informatiche.

mente riconosciute da tutti i tecnici del settore come base di partenza minima per il proficuo svolgimento delle operazioni di sequestro, analisi e conservazione di un supporto informatico.

Come detto, questa fase delle investigazioni informatiche, ed in particolare quella in cui il dato viene duplicato dal suo originale, risente, appunto, della fragilità e volatilità dello stesso, circostanza che impone l'adozione di particolari cautele.

Alla luce di quanto detto, tanto in fase di sequestro, quanto in fase di analisi e conservazione dei supporti o dei sistemi, l'operatore dovrà sempre redigere adeguata documentazione che tenga conto di tutte le operazioni compiute, riportate in ordine cronologico, in modo da permettere, anche in seguito, la ricostruzione dei vari passaggi attraverso i quali si è snodata l'attività di indagine.

Una volta identificati i sistemi o supporti da sequestrare, gli stessi dovranno essere inventariati e descritti in un apposito registro e dovranno essere imballati ed etichettati anche al fine di rendere sempre dimostrabile in dibattimento il rispetto delle procedure che riguardano la catena di custodia delle prove.

L'operatore dovrà, altresì, procedere ad effettuare uno o più duplicati dei supporti di memoria sequestrati, avendo cura di eseguire tale attività in modo che la stessa sia ripetibile innanzi al magistrato in sede dibattimentale.

La duplicazione del dato contenuto sui supporti costituisce uno dei momenti cardine delle investigazioni informatiche poiché è proprio nell'esecuzione di tale operazione che l'operatore deve fornire garanzia di non aver alterato le prove attraverso l'uso delle impronte digitali, o valori di Hash (22), che consentono di dimostrare che il duplicato corrisponde perfettamente all'originale.

È approccio comune di molti tecnici del settore quello di registrare, mediante l'uso di una videocamera, le attività effettuate per l'acquisizione della prova, al fine di consentire al magistrato ed alla difesa dell'indagato di prendere visione delle modalità di svolgimento delle indagini.

Una volta effettuati i duplicati il perito procederà all'analisi dei supporti per ricercare le informazioni necessarie alla ricostruzione dei fatti avendo cura che i dati estratti dai supporti soddisfino delle caratteristiche (23) minime quali l'autenticità, la ripetibilità, l'attendibilità.

(22) La codifica hash è un algoritmo che, partendo da un file o supporto di qualsiasi dimensione ed attraverso la sua elaborazione, produce un codice a dimensione fissa, detto «digest». Il funzionamento della codifica consente di sapere se un determinato file o supporto ha subito delle modifiche poiché il digest, in caso di alterazione del sorgente, presenta un valore differente da quello originale.

(23) SIGNORILE, *Computer forensics guideline: un approccio metodico-procedurale per l'acquisizione e l'analisi delle digital evidences*, *Cyberspazio e diritto*, Modena, vol. 10, 2009, 206 e ss.

Tale attività è spesso ostacolata dal sempre più diffuso uso di software o hardware che consentono di crittografare il contenuto dei supporti di memoria. In tutti i casi in cui il perito dovesse incontrare, nella ricerca del dato, intere aree di memoria o singoli file protetti o nascosti con tecniche di crittografia o altre tecniche di anti-forensics, lo stesso dovrà anche provvedere, quando tecnicamente possibile, a forzare le protezioni incontrate ed a relazionare dettagliatamente tutte le tecniche utilizzate per risolvere le difficoltà incontrate.

L'esperto, quindi, dovrà dimostrare che i dati recuperati non sono stati in alcun modo alterati e che le procedure adottate per la loro ricerca ed estrazione sono ripetibili da altro tecnico attraverso la descrizione dettagliata delle tecniche e dei software utilizzati per l'esecuzione dell'indagine. Appare opportuno evidenziare che qualunque attività del tecnico, nella maggior parte dei casi, sarà oggetto di severa verifica in sede dibattimentale.

Ogni procedura, gli strumenti ed i software adottati saranno oggetto di numerose eccezioni che ricadranno per lo più sulla trasparenza delle indagini, sulla loro ripetibilità e sulla corretta gestione del dato.

Nella redazione della perizia da consegnare al magistrato, pertanto, il perito dovrà far confluire tutta la documentazione necessaria a rendere sempre dimostrabile e verificabile l'attività eseguita attraverso l'allegazione delle caratteristiche tecniche ed operative di ogni software o hardware utilizzato, delle relative licenze d'uso e della documentazione che dimostri l'efficacia degli strumenti utilizzati in tale tipo di attività o indagine.

La mancata standardizzazione delle tecniche di computer forensics e la continua evoluzione della strumentazioni oggetto di indagine rende necessaria, quindi, l'adozione di procedure trasparenti che devono essere compiutamente descritte nella perizia ed anche attraverso una valutazione che deve sempre essere supportata da basi tecnico scientifiche.

Tali valutazioni dovranno sempre tenere in debito conto il contesto in cui la perizia dovrà essere utilizzata, ovvero quello dibattimentale, e dovranno perciò essere redatte in maniera chiara e rese comprensibili anche grazie all'uso di strumenti quali fotografie e video registrazioni che ritraggono la scena del crimine, il sequestro e la fase di analisi in laboratorio.