

GRUPPO DI INIZIATIVA FORENSE

Verona 7 maggio 2004

DOCUMENTO INFORMATICO

Problematiche

di formazione e probatorie

Gerardo Costabile

“Scena criminis, documento informatico e formazione della prova penale”

In una posizione particolare, non codificata e non sempre puntualizzata dalla dottrina o dalla giurisprudenza, si pongono le cosiddette “*prove digitali*”, in una sorta di “*metaterritorio*”, dove sembrerebbe perdere consistenza la naturale propensione dell’uomo di rapportarsi al mondo “*reale*” con l’uso dei cinque sensi e del tatto in particolare.

Questa pseudo-immaterialità nel processo di formazione della prova può dirsi strettamente correlata alla scarsa conoscenza del mondo “digitale”, ormai trasversalmente e prepotentemente presente simbioticamente nel mondo “reale”, tanto da rendere necessaria una nuova regolamentazione nel settore o, meglio ancora, l’aggiornamento di quella preesistente.

I computer e le altre apparecchiature elettroniche sono ormai presenti in ogni momento della nostra vita. L’uso dei nuovi metodi di comunicazione digitale, come ad esempio internet e le e-mail, ha drammaticamente incrementato l’ammontare delle informazioni che sono ordinariamente conservate e trasmesse solo in forma digitale. Questa evoluzione tecnologica ha però, contestualmente, agevolato e migliorato anche la commissione di vecchi e nuovi reati da parte della criminalità.

I computer, per questo motivo, possono essere i nuovi protagonisti nella commissione di reati, possono contenere le prove per crimini di tipo comune oppure possono essere essi stessi obiettivi di atti criminali. Ed è in tale contesto che si pone il *cyber-investigatore*, il quale ha l’esigenza e il dovere di valutare prima di tutto il ruolo e la natura delle “*impronte elettroniche*”, individuare quali supporti informatici possano contenere potenziali tracce nella *scena criminis*, acquisire e preservare

le stesse fino alla loro successiva analisi, laddove non fosse possibile espletare i dovuti accertamenti direttamente sul posto.

In Italia, purtroppo, non esiste formalmente una standardizzazione delle procedure e le modalità operative vengono demandate alla naturale professionalità degli operatori e della magistratura delegante, tentando affannosamente di non allontanarsi dalla sottilissima linea immaginaria, costituita dai quei principi generali del codice di procedura penale.

L'esperienza processuale ha però talvolta insegnato che è facile trasformare quella padronanza del *thema probandum* in un boomerang, vanificando in dibattimento tutta l'onerosa attività di indagine della fase preliminare.

Ma cosa sono realmente le tracce elettroniche, e particolarmente quelle informatiche? Non esiste una definizione codificata. In generale, quando si parla di "*digital evidence*" si vuole richiamare l'attenzione sulle informazioni ed i dati conservati o trasmessi dalle apparecchiature cosiddette digitali.

Queste tracce, come già accennato, sono caratterizzate da una foggia di immaterialità e per questa loro natura, per così dire aleatoria, possono essere considerate suscettibili alle impronte digitali oppure alle analisi del DNA. Ed è proprio a causa della loro fragilità che tali tracce possono essere facilmente alterate, danneggiate o distrutte, anche per colpa degli stessi investigatori o esaminatori non idoneamente preparati, con la conseguenza di fornire il fianco alla difesa dell'indagato, la quale potrà agevolmente infondere il dubbio alla magistratura giudicante sulla genuinità dell'iter di formazione della prova.

L'irreversibile passaggio dalla carta ai *bits* con la conseguente necessità di dimostrare in sede dibattimentale l'efficacia probatoria delle tracce informatiche e dei significati ad esse ascritti, pone alcuni interessanti interrogativi. Come possiamo garantire l'integrità di queste "*digital evidence*"?

Contrariamente a quanto si pensi, la sensibilizzazione per un comportamento corretto nel maneggiare le nuove tecnologie non è necessaria esclusivamente per le attività di accertamento dei reati informatici in senso stretto, ma appare di notevole importanza anche per quanto attiene altre tipologie di indagine, perfino di natura amministrativo-fiscale.

La cura del personale nell'esecuzione di indagini tipiche di polizia giudiziaria deve essere improntata alla protezione della *scena criminis*¹, al fine di assicurare l'integrità di tutte le prove, che siano esse di tipo tradizionale o elettronico-digitali.

La fase più delicata dell'azione di polizia giudiziaria, quando sono "trattate" informazioni digitali, è quella dell'acquisizione.

E' necessario, infatti, per evitare sgradite sorprese in fase dibattimentale e consentire eventuali perizie di parte su informazioni "genuine", che l'attività di analisi delle tracce informatiche sia operata non sull'originale del supporto sequestrato, ma su di una "immagine" dello stesso, consentendo in un secondo momento di effettuare una medesima attività a riscontro delle risultanze investigative ivi compendiate.

La "bit stream image", a differenza della mera copia, consentirà di operare su un hard disk praticamente identico all'originale, sia in maniera logica che fisica, quindi anche su eventuali parti presumibilmente vuote dello stesso, che potrebbero contenere *file* o frammenti di *file* cancellati non sempre visibili con i normali strumenti di *windows*².

Dovrà essere all'uopo effettuata tale operazione con idonei strumenti, hardware e software, che consentano di mantenere inalterata la traccia informatica oggetto dell'analisi, al fine di evitare dubbi sull'integrità dei dati contenuti nei supporti in parola e previo utilizzo di hard disk nuovo oppure assoggettato ad operazione di *wiper* (trattasi di rimozione dei dati molto approfondita con particolari programmi per evitare che possa essere recuperato un file cancellato riconducibile, ad esempio, al precedente utilizzatore del supporto usato).

Il sistema³, infine, dovrà operare in maniera non invasiva, ad esempio con l'ausilio di un blocco in scrittura, che consentirà di non compromettere l'integrità dei dati contenuti nel supporto oppure anche la mera variazione di un semplice orario di accesso ai file⁴, che non sarà ovviamente compatibile

¹ Marco Strano, Relazione alla Conferenza sul Cybercrime, Palermo, 3-4-5 Ottobre 2002, dove l'autore individua il *cyber-criminale* proiettato "in un contesto digitale, laddove la *scena criminis* (il luogo del delitto) si localizza tra i polpastrelli dell'autore e la tastiera, tra i suoi occhi e le emissioni elettromagnetiche del monitor".

² In tal modo viene anche preservata l'allocazione dei singoli file sul supporto originale. Infatti se vengono copiati i dati di un hard disk su un altro supporto idoneo, con un semplice procedimento di copia, i dati presenti in entrambe i dischi saranno uguali, ma sarà diversa la loro distribuzione.

³ Il software che ad oggi sembrerebbe quello più utilizzato per l'analisi in parola si chiama *EnCase*, prodotto dalla *Guidance Software*, destinato all'uso professionale ed investigativo da numerose agenzie e forze dell'ordine in tutto il mondo e considerato in linea con gli standard internazionali per le analisi delle tracce informatiche. Qualche critica è stata formulata dai promotori dell'*open source*, in quanto non sarebbero disponibili i codici sorgenti del software e quindi non sarebbe trasparente la procedura di *working* dell'analizzatore. Altri software di pregio utilizzati dagli esperti sono, tra gli altri, "SMART" e "Ilook investigator", quest'ultimo ad uso esclusivo delle forze dell'ordine, dei militari e delle agenzie governative su scala internazionale.

⁴ Per questo motivo è vivamente sconsigliabile l'accensione dei computer durante l'attività di sequestro, se lo stesso è spento. In tutti i casi comunque è indispensabile operare con la continua assistenza della parte, verbalizzando con precisione gli orari, tra i quali potrebbe essere importante riportare quello indicato dal computer stesso, evidenziando l'eventuale disallineamento.

con quello dell'avvenuto sequestro e quindi potrebbe compromettere l'eventuale non-ripudiabilità delle citate informazioni.

Nella formazione dell'immagine dovrà essere creata anche una sorta di impronta, che contraddistinguerà in maniera univoca la traccia informatica oggetto dell'analisi forense, al fine di ottemperare alle citate esigenze di integrità del dato. Tale "marchio digitale" sarà creato con un'operazione cosiddetta di *hashing* a senso unico, con algoritmo di classe MD5, che genera un'impronta della lunghezza di 128 bit (16 byte). L'impronta costituisce un riferimento certo alla traccia originale, ma non ne consente la ricostruzione. Tale algoritmo è utilizzato a livello internazionale e garantisce un buon livello di sicurezza. Difatti la probabilità di avere la medesima impronta per due documenti differenti, anche se solo di una virgola, è pari a 2 elevato alla 128[^] potenza, ovvero sarebbe ad esempio come vincere il granpremio americano della lotteria Powerball per 39 volte di seguito.

Più in generale il mondo giuridico e giudiziario appare diviso sulla necessità o meno di acquisire tutto il supporto informatico nella fase di sequestro penale. Molteplici sono state le posizioni, più o meno condivise dalla giurisprudenza, di coloro che indicavano come oggetto del sequestro non il contenitore in se, ma i dati informatici ivi contenuti. Le critiche più articolate, da parte della dottrina⁵, hanno preso le mosse da un attento esame dell'istituto del sequestro probatorio, approfondendo le nozioni di corpo del reato e cose pertinenti al reato. Infatti l'art. 253 comma 2 cpp indica quale corpo del reato quelle cose sulle quali o mediante le quali il reato è stato commesso, includendo altresì quelle che ne costituiscono il prodotto, il profitto o il prezzo.

Secondo la citata dottrina, non sarebbe conciliabile la definizione marcatamente materiale del legislatore con la natura immateriale delle tracce informatiche⁶.

D'altro canto la giurisprudenza non sembra aver dato adeguate risposte, riconoscendo alternativamente ad un computer⁷ la qualità di corpo del reato, ovvero il mezzo attraverso il quale viene consumata l'azione criminosa, oppure di cosa pertinente al reato, in quanto elemento esterno dell'*iter criminis*, con l'esame del quale può essere dimostrato il fatto criminoso, comprese le modalità di preparazione ed esecuzione⁸.

E' palese che tale vincolo pertinenziale non sembra sussistere sempre tra il reato e l'intero supporto informatico, in luogo delle sole tracce ivi contenute, almeno nei casi in cui il computer non può essere semplicisticamente considerato come "l'arma del delitto".

⁵ Cfr. Francesco Marcellino, Principio di pertinenza e sequestri di computer, disponibile su www.netjus.org.

⁶ L'immaterialità del dato informatico è stata riconosciuta dallo stesso legislatore il quale, tra i computer crimes, non ha previsto il reato di furto, limitandosi alla mera duplicazione abusiva.

⁷ Cfr. Cass. Pen. Sez. VI, 29 gennaio 1998.

⁸ Cfr. Cass. Pen. Sez. V, 22 gennaio 1997, n. 4421.

Per questo motivo appare fondamentale valutare il “ruolo” del computer nell’attività illecita, per motivarne l’eventuale sequestro.

In generale infatti l’hardware di un computer può essere osservato sotto due distinti profili. Il computer, e non solo quello ovviamente, può assumere la veste di mero contenitore della prova del crimine, ad esempio può immagazzinare il piano di una rapina o le mail intercorse tra i complici. In tal caso non sarà necessaria un’azione di sequestro, ma potrà essere operata in contraddittorio una semplice masterizzazione delle tracce pertinenti al reato, con lo strumento di polizia giudiziaria più appropriato, come ad esempio un’ispezione delegata ex art. 246 cpp.

L’ispezione è una particolare attività tipica di polizia giudiziaria volta all’esame di persone, cose o luoghi, allo scopo di accertare le tracce e gli altri effetti materiali del reato (ad esempio impronte sul pavimento, macchie di sangue).

Questa attività di polizia giudiziaria, poco utilizzata nel settore dei reati informatici in quanto esigente di specifiche competenze tecniche e variegato materiale software, è caratterizzata dall’irripetibilità degli atti, con la conseguente utilizzabilità piena originaria nel dibattimento.

Tale procedura, molto incoraggiata da parte della dottrina, appare consigliabile esclusivamente per piccoli reati (ad esempio in presenza di *dialer*, diffamazione, *virus*), in quanto, come già accennato, si tratta di un’attività particolarmente tecnica dove l’operatore deve, in contraddittorio con la parte, “esplorare” i supporti informatici dell’indagato, (o talvolta dello stesso esponente) alla ricerca di dati e tracce informatiche inerenti i fatti oggetto dell’ispezione, che saranno cristallizzati con i dovuti metodi in supporti durevoli allegati al verbale.

Pare meritevole ivi segnalare due limiti: uno di natura meramente temporale, in quanto non è sempre possibile analizzare sul posto una grande mole di dati, considerando anche quelli cancellati che dovranno, ove possibile, essere opportunamente recuperati.

Un altro problema invece è l’impossibilità, da parte dell’indagato, di esperire in un secondo momento una nuova analisi ad opera di un perito di parte, in quanto il supporto prodotto in sede di ispezione, oppure l’hard disk stesso oggetto dell’attività, non saranno i medesimi sui quali il “cyber-investigatore” aveva operato⁹.

Dovrà quindi essere valutata preventivamente l’opportunità dell’ispezione, consigliabile preferibilmente quando un sequestro indiscriminato sarebbe sproporzionato al fatto contestato, ovvero quando l’hard disk è stimabile solo come contenitore di documenti informatici inerenti alle indagini, oppure nel caso di attività presso terzi (banche, provider, etc.) estranei di fatto alla vicenda.

⁹ In realtà tali operazioni di polizia giudiziaria non sono quasi mai oggetto di contestazione immediata da parte dell’indagato il quale, specialmente per reati comuni, non sempre ha la competenza tale per poter contraddire un processo di estrapolazione dei dati, condizionato talvolta anche da una sorta di timore reverenziale.

In altri casi, invece, l'hardware può essere considerato come frutto dell'attività criminale, come ad esempio il contrabbando, oppure uno strumento per la commissione di reati.

Un computer utilizzato per consumare il reato di cui all'art. 615 ter cp (accesso abusivo ad un sistema informatico) potrebbe quindi essere annoverato tra gli strumenti per la commissione del crimine. In America, in questi casi, il *Federal Rule of Criminal Procedure n. 41* consente agli agenti, previo decreto, il sequestro dell'intero hardware, qualunque sia il materiale ivi contenuto. Successivamente sarà effettuata la *digital analysis* del contenuto delle risorse informatiche dell'indagato.

Paradossalmente in Usa sarebbe possibile sequestrare un'intera rete informatica laddove fosse accertata la commissione di un reato ad opera di un amministratore di rete nell'esercizio della propria attività¹⁰.

Negli altri casi, cioè quando l'hardware è un mero contenitore, le procedure federali d'oltreoceano danno maggiore rilevanza al sequestro del dato informatico, ritenuto centrale rispetto all'indagine, rispetto all'hardware che lo contiene. Ciò non vuol dire che il sequestro *tout court* degli hard disk sia vietato, ma viene valutata caso per caso la fattibilità in determinate circostanze "informatiche", ovvero quando la mole di dati è di un certo spessore¹¹, oppure si ha motivo di ritenere che ci siano file nascosti, stenografati, crittografati, non allocati, ovvero sistemi di autodistruzione dei dati in caso di password errata, etc.

La risposta più adeguata alle problematiche sopra evidenziate sembrerebbe essere il buon senso, ossia garantire una blindatura delle procedure e della relativa *chain of custody*, utilizzando lo strumento giuridico più adatto, motivando adeguatamente la sussistenza delle concrete esigenze probatorie con riferimento, cioè, alla "pertinenza" probatoria delle cose eventualmente sequestrate o oggetto di ispezione, in relazione alle quali andranno indicati gli elementi di fatto specifici che giustificano il provvedimento¹².

Dovrà quindi essere individuato¹³ compiutamente il *thema probandum*, ovvero il fatto storico e concreto riconducibile, almeno astrattamente, ad una fattispecie criminosa. In mancanza di tale individuazione non sarebbe possibile accertare né l'esistenza delle esigenze probatorie su cui si fonda il provvedimento, né la natura di corpo del reato o cosa ad esso pertinente, oggetto di ricerca

¹⁰ Trattasi di una facoltà in capo alla polizia giudiziaria americana. Anche in Italia è guardata con più rigore l'opera criminale dell'amministratore di sistema, il quale è punito più severamente in caso ad esempio di accesso abusivo ex art. 615 ter cp.

¹¹ Questo è il caso più frequente in quanto l'attività di estrapolazione o di *bit stream image* può essere onerosa, dal punto di vista temporale, e in taluni casi può essere più invasiva dell'asportazione dei supporti informatici, che potranno essere "copiati" in laboratorio.

¹² Cfr. Cass. Penale n. 649 del 2 marzo 1995.

e acquisizione. In tal caso quindi la perquisizione non sarà più un mezzo di ricerca della prova, ma un discusso mezzo di acquisizione della *notitia criminis*¹⁴.

Tale indeterminatezza, accompagnata dall'indicazione che potrà essere oggetto di sequestro "quanto ritenuto utile ai fini dell'indagine", rimetterebbe alla polizia giudiziaria la valutazione e l'individuazione dei presupposti fondamentali del sequestro¹⁵, con la spiacevole conseguenza, non avendo ben precisato l'importanza di taluni dati in luogo dell'intero supporto e non avendo valutato la possibilità di un'ispezione delegata, di "agevolare" un sequestro indiscriminato di corposo hardware, contenente dati anche di terze persone e quindi poco inerente¹⁶. Infatti appare palese la multifunzionalità dei supporti informatici, difficilmente vincolati nella loro interezza all'attività illecita¹⁷.

Il sequestro del bene informatico deve pertanto essere valutato caso per caso e non in maniera superficiale, attesa la molteplice destinazione e funzione dello strumento.

Tale impostazione impone un più rigoroso accertamento sulla sussistenza delle finalità probatorie e sugli strumenti tecnico-giuridici più idonei all'attività di cristallizzazione ed assicurazione della prova informatica, **garantendo altresì certezza, genuinità e paternità ai dati informatici**, evitando contestualmente conseguenze altamente afflittive e interdittive, ancorché lesive ed estranee alle esigenze d'indagine¹⁸.

Appare d'obbligo infine citare, proprio nel codice penale, l'art. 491 bis dove si legge, tra l'altro: *"omissis... A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli"*. Quindi, testualmente, la distinzione tra il documento cartaceo e quello informatico consiste tutta nel supporto contenente i dati: questi, infatti, viene indicato quale equivalente

¹³ Cfr. Arrigo Daniele, Il riesame della perquisizione e del sequestro penale mancanti dell'indicazione del thema probandum, 1999, n. , p.823, Giurisprudenza Italiana a commento di Cassazione VI Sezione, 26 marzo 1997.

¹⁴ Cfr. Cassazione VI Sezione, 26 marzo 1997, che ritiene "insufficiente quale enunciazione, ancorché sommaria e provvisoria, d'ipotesi accusatoria, la mera indicazione, nei provvedimenti di perquisizione e sequestro, degli articoli di legge pretesamente violati, seguiti da una collocazione spazio-temporale così ampia da non apportare alcun contributo alla descrizione del fatto".

¹⁵ Cfr. "Decreti di perquisizione e sequestri ex art. 252 cpp: limiti e discrasie" - Avv. Alfonso Maria Parisi, Patrocinante in Cassazione, su www.penale.it.

¹⁶ L'indeterminatezza dell'indicazione ha come conseguenza diretta la necessità, secondo parte della giurisprudenza (Cfr. Cass. Pen., V, 17 marzo 2000), di una convalida ex art. 355 cpp.

¹⁷ Il Tribunale di Torino, con un notorio provvedimento del 7 febbraio 2000 in materia di sequestro probatorio di hard disk, pur non accogliendo le eccezioni sull'asserita immaterialità delle tracce informatiche, ha ordinato il dissequestro dell'hardware, riconoscendo altresì che questi è cosa pertinente al reato, ma asserendo che le esigenze probatorie potevano essere garantite con l'estrazione dei soli dati oggetto dell'attività illecita, in quanto l'intero supporto conteneva anche informazioni riferibili alla corrispondenza telematica tra l'indagato e terzi, totalmente estranei ai fatti.

¹⁸ Cfr. Cassazione penale, sez. III, 25 febbraio 1995, n. 105, e Tribunale del riesame di Torino, 7 febbraio 2000.

informatico del tradizionale foglio di carta, sul quale un contenuto eventualmente rappresentativo può essere impresso¹⁹.

Questo spinge a valutare l'attività di assicurazione della prova sempre più nella direzione della cristallizzazione del contenitore in luogo del suo contenuto, mentre nel caso dell'informatica le due cose sono facilmente scindibili, pur assicurando medesimo risultato. In conclusione, quindi, se pure da un lato è possibile l'applicazione di un idoneo accorgimento tecnico, rispettoso dei principi costituzionali e garanzia della genuinità della prova, è auspicabile un aggiornamento delle procedure del codice di rito, al fine di svincolare alcune terminologie dall'impostazione profondamente ancorata alla materialità degli eventi²⁰.

Mentre tale obiettivo, seppure lontano, appare più chiaro e definito all'orizzonte, tanto che anche alcune Università in Italia (cito, per conoscenza personale, **l'Università di Milano con il Prof Ziccardi e quella di Bologna con il Prof. Maioli**) si stanno facendo promotrici, in ambiente certamente scientifico, di progetti di linee guida per le attività di computer e network forensics²¹, le attività sono spesso poco omogenee e gli interventi non sempre proficui, oltre che spesso in pregiudizio di alcuni principi fondamentali dell'individuo.

¹⁹ Leggasi l'interessante articolo su <http://www.romagna-camerapenale.it/docinformatico.htm> relativo al documento informatico.

²⁰ Tale impostazione è stata già applicata per dipanare un problema analogo afferente il reato di furto ex art. 624 cp, ove è stata parificata a "cosa mobile anche l'energia elettrica e ogni altra energia che abbia valore economico".

²¹ L'accezione "Computer Forensics" si riferisce a quella disciplina che si occupa della preservazione, dell'identificazione, dello studio, della documentazione dei computer, o dei sistemi informativi in generale, al fine di evidenziare prove per scopi di indagine.