STEFANO ATERNO - FRANCESCO CAJANI
GERARDO COSTABILE - DONATELLA CURTOTTI

CYBER FORENSICS E INDAGINI DIGITALI

Manuale tecnico-giuridico e casi pratici

prefazione di
Giorgio Spangher e Filippo Spiezia

G. Giappichelli Editore

IL FUTURO CI HA RAGGIUNTO

Il futuro ci ha raggiunto. Era prevedibile ed era anche previsto. Incerti i tempi. L'emergenza sanitaria li ha solo accelerati e fortemente materializzati. Siamo prepotentemente entrati nell'era digitale e conseguentemente nella predisposizione degli strumenti per garantire lo sviluppo in condizioni di sicurezza al fine di sfruttarne al meglio le potenzialità. A fianco alle potenzialità positive i nuovi strumenti informatici consentono di sviluppare anche quelle negative, deviate e patologiche, sia in se, sia in quanto oggetto di attività criminali. Non eravamo del tutto impreparati, ma le questioni si sono prepotentemente dilatate prospettando aspetti complessi spesso collocati in territori sconosciuti, sia nelle questioni, sia nelle possibili soluzioni.

Il dato non può prescindere dal raccordo con le nuove fattispecie incriminatrici che si vengono progressivamente delineando nella costruzione dell'attività di contrasto alla criminalità informatica, nella sua dimensione costantemente, velocemente, camaleonticamente modificata e nella articolazione globalizzata, diffusa, sfuggente, soprattutto considerando la sua immateriale materialità.

Considerato il grande rilievo dei beni da proteggere, non manca la predisposizione di misure sicuritarie di prevenzione e di protezione molto complesse ed esse stesse in costante adeguamento e perfezionamento.

Si colloca in questo contesto il primo autentico Manuale di *cyber forensics* e di indagini digitali, capace di scandagliare una materia solo apparentemente arida e fredda, nella quale invece si annida la vita della società in evoluzione.

Dopo aver delineato e definito i profili tecnici di base, cioè il nuovo lessico della materia, l'analisi approfondisce i rapporti tra le prove digitali e gli sviluppi processuali secondo le stesse scansioni del codice di rito penale.

Anche in questo caso, infatti, come in tutte le vicende processuali, il tema centrale è costituito dalla prova, dalle modalità di formazione, di acquisizione, di conservazione e di valutazione.

Il valore aggiunto del lavoro consiste proprio nella capacità di affrontare la tematica della legalità della "nuova" prova digitale, evitando le facili scorciatoie connesse alla mancanza di riferimenti normativi e alla necessità di efficaci strumenti di contrasto a fenomeni criminali di accentuata pericolosità.

In altri termini, la ricostruzione dei percorsi e degli strumenti a disposizione degli organi investigativi non può prescindere da detta necessità di intersecarsi con le garanzie proprie di un giusto processo. In quest'ottica si colloca il punto di forza del lavoro, nella capacità, cioè, di declinare il tema investigativo della prova digitale secondo lo schema di un metodo rispettoso dei diritti costituzionali e sovranazionali.

Un viaggio nella molteplicità dei profili pratici – operativi ai quali sono fornite risposte che saranno di orientamento per le soluzioni che dovranno essere proposte dagli operatori del diritto.

Si conferma quell'interazione con la tecnicità e "scientificità" che il processo sta sempre più assumendo, nella quale si profila indispensabile la presenza del consulente della prova, nel contesto della dialettica dei saperi, capace di fornire al giudice il supporto per le sue decisioni.

Giorgio Spangher
Professore Emerito di Procedura penale
Università degli studi di Roma "La Sapienza"

CYBERCRIME, L'ULTIMA FRONTIERA

Negli ultimi decenni la tecnologia digitale ha trasformato profondamente le nostre società ed il modo di vivere, facilitando le relazioni sociali e la circolazione di dati (personali e non). Si tratta di cambiamenti straordinari. Persino il concetto di lavoro a cui eravamo abituati risulta modificato.

La grave pandemia conseguente alla diffusione del COVID – 19 fornisce l'ultima eloquente conferma: accanto ai suoi profili sanitari e alla minaccia per la salute di milioni di persone, essa verrà probabilmente ricordata per aver innestato un ulteriore salto – quantitativo e qualitativo – nel ricorso diffuso alla rete.

Quest'ultimo ha attenuato alcuni degli effetti derivanti dalle misure di "distanza sociale" applicate su scala globale. La nostra quotidianità è stata più basata sul "ciberspazio", quale luogo da cui ormai dipendono le nostre interazioni sociali oltre che la nostra economia.

Abbiamo apprezzato alcuni dei vantaggi offerti da *Internet.* Essi non possono essere messi in discussione. Accanto a questi, tuttavia, il mondo digitale ha dato vita ad una nuova categoria di minacce. L'utilizzo illecito della tecnologia ha generato la criminalità cibernetica, fenomeno in continua espansione, che aumenta con l'avanzare dello sviluppo tecnologico e rende i cittadini, le imprese e gli Stati particolarmente vulnerabili.

Secondo i dati raccolti nel 2017 dal *Norton Cyber Security Insights Report,* 978 milioni di *consumers*, provenienti da 20 paesi diversi in tutto il mondo, sono stati colpiti da attacchi di tipo informatico (fra cui circa 16 milioni solo in Italia). Tra le vittime, una speciale preoccupazione per i minori: sono proprio i bambini e gli adolescenti ad essere esposti maggiormente a reati informatici particolarmente pericolosi, primo fra tutti lo sfruttamento sessuale online. Secondo i dati raccolti da Europol i minori rappresentano all'incirca il 70% del totale delle vittime che vengono annualmente soggette a ricatti di tipo sessuale online.

Quelle appena riportate sono cifre allarmanti, che danno conto dei livelli di pervasività e diffusività che gli attacchi informatici possono raggiungere.

Negli ultimi anni, si è assistiti ai primi attacchi hacker a livello globale. In particolare, gli attacchi *WannaCry* e *NotPetya* hanno dato l'idea di come il cybercrimine possa colpire vari strati della società, perturbando la fornitura di servizi es-

senziali: nel giro di pochi giorni, fra il maggio e il giugno 2017, questi *ransomware* hanno colpito più di 300.000 utenti in 150 diversi Paesi, infettando i sistemi di molte aziende e istituzioni europee di rilevante interesse sociale, come la Deutsche Bahn in Germania e il National Health Service nel Regno Unito.

Entro il 2030, è previsto che saranno 125 miliardi gli oggetti connessi ad internet e che il 90% dei soggetti al di sopra dei 6 anni di età saranno online. L' "Internet delle cose" (*Internet of Things*), ossia quella dimensione in cui vari oggetti (quali televisori, elettrodomestici, automobili, etc.) sono connessi ad Internet, è una realtà a cui siamo già ben avvezzi. In un tale contesto, il numero delle vittime potenziali del cybercrimine è destinato ad aumentare.

L'esperienza investigativa condotta negli ultimi anni, dalle autorità nazionali e dalle agenzie europee, inclusa Eurojust, dimostra che, nella maggior parte dei casi i cyber-attacchi e, in generale, i reati informatici, non sono espressione di condotte criminali isolate, bensì il frutto dell'attività di organizzazioni criminali, più o meno strutturate, che si avvalgono di ingenti risorse umane e finanziarie (si stima che il costo globale del cybercrimine sia di circa 530 miliardi di euro).

Le organizzazioni criminali sono attratte dalle potenzialità che la tecnologia offre, poiché l'uso di Internet permette loro di massimizzare i profitti, sfruttando strumenti nuovi per perpetrare "vecchie" condotte. L'esperienza dei mercati illegali nel *Dark Web* è emblematica in tal senso: attraverso il ricorso al "lato oscuro" di Internet, i cybercriminali hanno trovato una nuova dimensione al traffico illecito di droghe e di armi.

Fra gli attori che più si servono delle potenzialità del mondo digitale vi sono, poi, le organizzazioni di tipo terroristico.

L'utilizzo di siti web, di social networks o di forum e piattaforme online per alimentare il credo jihadista, ha portato all'avvento di una nuova era, quella del terrorismo digitale di massa, in cui i gruppi terroristici vedono nel Web l'opportunità per mantenere il controllo e la resilienza, anche quando incontrano ostacoli nella realizzazione del progetto di costruzione di uno stato territoriale.

Stare al passo con la criminalità sul versante investigativo è un'operazione alquanto difficile, per diverse ragioni. Una delle sfide della cybercriminalità deriva dalla sua "*a-territorialità*": i reati informatici, per definizione, non conoscono confini. Infatti, lo spazio virtuale è uno spazio unitario, che sfugge dal dominio di un solo Stato e in cui le norme sulla ripartizione della competenza territoriale comunemente applicate non sono utilizzabili.

Accanto ad essa, si situa la continua evoluzione di metodi criminosi che si basano sullo *sfruttamento della vulnerabilità umana*. La diffusività ed invasività dei cyber-attacchi è garantita sempre più da sofisticate tecniche di *social engineering*

utilizzate da parte dei gruppi hacker. Esempio di tale sviluppo è quello del BEC Fraud (*Business Email Compromise Fraud*), che consiste in un'abusiva intercettazione di email che vengono scambiate dalle unità di alto livello all'interno delle organizzazioni delle imprese – che normalmente utilizzano un sistema di software (Microsoft 365) – con cui dettano gli ordini di pagamento agli uffici inferiori.

Ma una vera propria sfida nella sfida risiede nelle difficoltà di accesso legale *ai dati* digital, che costituiscono le prove utilizzabili per risalire agli autori di reato ed ottenerne l'incriminazione.

La prova digitale (*e-evidence*) nelle sue molteplici sfaccettature – dalla sua definizione forense, alle modalità di raccolta, anche in ambito transfrontaliero ed analisi, in vista del successivo utilizzo – è al centro di questo aggiornato e completo manuale.

L'Opera degli Autori è davvero meritoria. Essa si segnala per la sua completezza, per il rigore scientifico, per l'aggiornamento dei suoi contenuti. Si tratta di uno strumento indispensabile per ogni giurista ed operatore chiamato a svolgere attività e funzioni in materia.

Il testo ci aiuta a muoversi su una prospettiva razionale, l'unica possibile, che vede nello sviluppo della tecnologia non solo una possibile fonte di pericolo, ma anche un ambito scientifico e culturale di cui esplorare tutte le potenzialità, in vista di una consapevole difesa rispetto alle minacce poste dal crimine informatico.

Mentre è dunque auspicabile che vadano in porto le diverse iniziative, a livello normativo, per risolvere punti nodali della prova digitale, legati alla sua intrinseca transnazionalità ed immaterialità – mi riferisco al Progetto sulla e-*Evidence*, portato avanti dalla Commissione europea ed alle iniziative per la definizione di una cornice legale comune in materia di *data retention* – resta ancora tanta strada da percorrere, per accrescere il livello della formazione professionale di magistratura, avvocatura e polizia giudiziaria, nonostante grandi progressi siano compiuti.

Si tratta di un traguardo alla portata. Ad esso dovranno puntare in modo sempre più convinto le istituzioni di formazione nazionale ed europea.

L'impresa è complessa, sia per la vastità della materia che per la rapida obsolescenza dei suoi contenuti che risentono intimamente delle evoluzioni della ricerca scientifica e tecnologica. Non si tratta di compito impossibile: oggi sappiamo di poter contare, nell'attuazione di questo obiettivo essenziale, anche su questo nuovo volume, che costituisce prezioso, indispensabile strumento.

Anche per questo mi sento di esprimere un sincero ringraziamento agli Autori.

Filippo Spiezia
Magistrato, Vicepresidente di Eurojust

Capitolo 1

DIGITAL FORENSICS & DIGITAL INVESTIGATION: CLASSIFICAZIONE, TECNICHE E LINEE GUIDA NAZIONALI ED INTERNAZIONALI

Gerardo Costabile

1. Digital forensics & digital investigation: definizioni e punti di attenzione

Se la digital evidence può definirsi, di fatto, la misura atomica delle indagini nel mondo digitale, la digital forensics può definirsi come un **processo teso alla "manipolazione controllata" e più in generale al trattamento** di dati e/o informazioni digitali e/o sistemi informativi per finalità investigative e, più in generale, di giustizia [1], adottando procedure tecnico-organizzative tese a fornire adeguate garanzie in termini di integrità, "autenticità" e disponibilità delle informazioni e dei dati in parola.

Inutile dire che tale disciplina, secondo alcuni chiamata anche informatica

[1] Per un'analisi delle varie definizioni, si rimanda a G. ZICCARDI, *Scienze forensi e tecnologie informatiche*, in AA.VV., *Investigazione penale e tecnologia informatica*, a cura di L. LUPARIA-G. ZICCARDI, Milano, 2007, 3 ss.

forense, non può limitare il proprio raggio d'azione alle sole indagini relative ai c.d. reati informatici, essendo di aiuto all'intero mondo delle investigazioni nel settore penale.

Si cominci col dire che esiste una differenza tra l'"**informatica forense**" e la "**sicurezza informatica**", seppure le due aree di attività siano strettamente collegate tra loro.

Si può pensare alla sicurezza informatica, da un lato, come elemento di ostacolo e, dall'altro, come fonte di strumenti ed opportunità per l'informatica forense. Infatti, la sicurezza informatica ha come proposito finale l'avvicinarsi alla realizzazione di sistemi il più possibile sicuri, ma qualora tale grado di sicurezza venisse elevato (ad esempio, da parte del responsabile di un illecito)[2], allora – per definizione – dal sistema sarebbe più complicato estrarre il desiderato contenuto informativo. L'acquisizione dei reperti informatici richiederà, in tal caso, la "violazione" del sistema oggetto dell'analisi, ed in questo campo la stessa sicurezza informatica sarà d'aiuto, in quanto fonte di studi sulle tecniche di hacking (utili per realizzare l'accesso alle informazioni protette) e sulla loro applicazione pratica. Inoltre, le "best practice" di sicurezza definiscono molti requisiti sui sistemi che, se opportunamente applicati, potranno in un secondo momento rendere disponibili un gran numero di informazioni aggiuntive, utilizzabili per l'analisi forense (si considerino, ad esempio, i log sugli apparati connessi ai sistemi da analizzare, i controlli di accesso, ecc.).

Nel linguaggio comune, per **digital forensics** s'intende anche il processo investigativo mediante il quale si utilizzano tecniche informatiche atte a raccogliere elementi probatori di varia natura (ad esempio, l'intestatario di una linea dati o di un sito web), oppure a fornire strumenti utili all'investigatore (nei casi più semplici, ricerca di informazioni sul web come una fotografia dell'indagato oppure l'identificazione di un latitante che usa imprudentemente Facebook, Twitter o altri social network; in quelli più complessi, uso di sistemi di business Intelligence finalizzati alle correlazioni non dirette tra persone, telefonate, sospetti, informazioni).

In un mondo sempre più digitale, il rischio di "allargamento" di questa definizione potrebbe indurre gli studiosi ad "abusare" del ruolo di tale disciplina nei vari contesti investigativi, spostando di fatto il baricentro a favore dell'informa-

---

[2] In tal caso si può parlare anche di "**antiforensics**". L'antiforensics è, comunque, una tecnica tesa all'occultazione o alla falsificazione dei dati da parte dell'indagato (prima ovviamente della perquisizione), con lo scopo di "distrarre" o indurre in errore gli investigatori. Per un maggior dettaglio si rimanda a D. GABRINI, *Aka Rebus*, in *http://informaticagiuridica.unipv.it/convegni/2007/pdf/Gabrini.pdf*. Cfr. anche A. GHIRARDINI-G. FAGGIOLI, *Computer Forensics*, Milano, 2007, 349 ss.

tica la quale, invece, è opportuno che rimanga il più possibile neutra ed "al servizio" di questa o di altra materia.

Di qui, si potrebbe definire una "nuova" disciplina dal nome "**digital investigation**" o "**informatica investigativa**", sorella della digital forensics e cugina della più nota informatica giuridica.

Il rischio di tecno-centrismo [3], che ha appassionato molti studiosi (tecnici e giuristi) negli ultimi 10 anni, ha portato talvolta a confondere i ruoli all'interno di alcuni processi sui reati informatici. Negli anni è accaduto, ad esempio, che alcuni giuristi, dotati di alcune competenze di computer forensics, abbiano tentato di proporre modificazioni delle fonti di prova digitale, senza però definire (preferibilmente se non necessariamente con l'ausilio di un consulente tecnico) dove e come le stesse avrebbero avuto origine e conseguenza. Questa sorta di "accanimento informatico", ad avviso di chi scrive, ha – più spesso in passato – fatto perdere la lucidità e la visione d'insieme di tutti gli elementi processuali, limitando l'analisi alle mere dissertazioni informatiche, con il rischio di farsi trascinare, addirittura, ad ammettere senza volere certe delucidazioni tecniche dell'accusa [4]. Questo rischio, altresì, ha ragione d'essere evidenziato per quanto

---

[3] L. LUPARIA, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in AA.VV., *Investigazione penale e tecnologia informatica*, cit., 136, dove si rimarca il rischio di una "deriva tecnicistica": "[D]del resto, per quanto sia innegabile che i nuovi settori dell'investigazione pongono sempre l'interprete in uno stato di smarrimento per le difficoltà correlate al loro collocamento tra i paradigmi teorici che compongono il tradizionale bagaglio culturale del processualpenalista (a dinamiche similari si è assistito in tema di riprese visive e rilevazioni GPS), è altrettanto vero che, il più delle volte, i princìpi consolidati della teoria processuale possono essere sufficienti per risolvere le questioni connesse al nuovo fenomeno delle indagini informatiche e che, anzi, l'eccessivo scostamento dallo *ius commune iudiciale*, perseguito da chi sostiene la bandiera di quella presunta "autonomia sistematica" delle operazioni di computer forensics, finisce col provocare pericolosi scostamenti tecnicisti e fenomeni di aggiramento delle garanzie processuali". Più in generale, D.L. FAIGMAN, *Legal Alchemy: The Use and Misuse of Science in the Law*, New York, 1999; A. CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen.*, 1999, 1192 ss.; F. CAPRIOLI, *Riprese visive nel domicilio e intercettazione "per immagini"*, in *Giur. cost.*, 2002, 2176 ss.; F. RUGGIERI, *Riprese visive e inammissibilità della prova*, in *Cass. pen.*, 2006, 3937 ss.; A. SCAGLIONE, *Attività atipica di polizia giudiziaria e controllo satellitare*, in *Foro it.*, 2002, II, 635 ss.

[4] Si riprende, a mero titolo di esempio, un passaggio del Tribunale di Bologna, sentenza 21 luglio 2005, relativo al processo c.d. Vierika: "[L]le attenzioni della difesa, nella memoria depositata alla udienza del 23/6/04, si sono concentrate sul fatto che il programma interagisce solo con Outlook e non con la più diffusa versione Outlook Express; su correzioni terminologiche (come il riferimento improprio ai programmi 'sorgente' sequestrati all'imputato) o sulle valutazioni del teste F., in particolare in ordine alla potenziale diffusività del programma; sulle generalizzazioni ed esemplificazioni contenute nelle note di polizia giudiziaria. Dalle stesse considerazioni della difesa si ricava, peraltro, che Vierika è un codice autoreplicante in due parti […] in grado di infettare […] le macchine con Windows 95 o 98 con istallato il software 'Outlook Professional'della

concerne gli investigatori. Sempre più spesso, purtroppo, si registrano "semplificazioni investigative" (principalmente per i c.d. reati informatici), che portano ad eludere le metodologie tradizionali di riscontro, pedinamento, osservazione *et similia*. Addirittura, in taluni casi, in spregio a tutte le prassi e le regole, si sono registrati casi di richieste di rinvio a giudizio senza neppure aver effettuato una perquisizione, senza aver avuto la conferma (o meno) che una determinata condotta sia stata realmente operata dall'intestatario della linea telefonica o invece, come spesso accade, da un altro familiare. Etica [5], garanzie, professionalità e più in generale qualità delle indagini a tutto tondo, dovrebbero essere la spina dorsale di un settore che, invece, si lascia spesso condurre da coloro che prediligono "indagare" solo di fronte ad un pc o in un laboratorio, sottovalutando gli schemi "classici" della cultura investigativa [6].

---

piattaforma 'Microsoft Office'". Si legge ancora che "se andiamo a leggere il codice di Vierika, troviamo che esso chiama funzioni dell'interfaccia MAPI completa, in particolare per acquisire gli indirizzi dalla rubrica". Inoltre, si contesta la sussumibilità delle impostazioni di protezione di Internet Explorer nel concetto normativo di misure di sicurezza, ma non che il programma apponesse tali modifiche, tanto più che – si spiega – per ripristinare le impostazioni originarie sarebbero bastati "quattro click del mouse"; si contesta la ingannevolezza del messaggio e-mail portatore del programma, ma non il fatto che abbia una doppia estensione e contenga un codice eseguibile; si contesta che il programma abbia un funzionamento di tipo "troiano" con appropriazione e diffusione di dati riservati, ma si ammette che esplica "funzioni di mailing del software Outlook installato sulla macchina al fine di autoreplicarsi". Poi, si riconosce che "Vierika è un worm che si autodiffonde utilizzando gli indirizzi di posta elettronica e che si manifesta come allegato di posta elettronica". Per quanto concerne la visione d'insieme delle fonti di prova, si riporta quanto invece indicato dalla Corte d'Appello di Bologna, sez. II, 27 marzo 2008**,** n. 369, per cui "[N]non si vede come possa esser messa in dubbio la fidefacienza di una risultanza documentale (tale è la traccia telematica, seppur necessitante di appositi strumenti per la fruibilità), coincidente con le ammissioni dello stesso imputato".

[5] Cfr. G. ZICCARDI, *Scienze forensi e tecnologie informatiche*, cit., p. 25, ove si legge: "[U]un auspicabile momento di approfondimento, all'interno della forensics, potrebbe riguardare gli aspetti etici: la computer ethics potrebbe essere affiancata, in tal caso, da una forensics ethics, ovvero da un'analisi rigorosa dei principi etici che devono muovere ogni soggetto che analizzi dati a fini investigativi".

[6] Secondo Cass, sez. IV, 10 gennaio 2002, n. 734, in *CED Cass*., n. 220944, "è legittimo, una volta ottenuto con il sequestro la disponibilità di un telefono cellulare costituente mezzo per la commissione del reato (nella specie relativo a spaccio di stupefacenti), che l'operatore di polizia giudiziaria risponda alle telefonate che pervengono all'apparecchio ed utilizzi le notizie così raccolte per l'assunzione di sommarie informazioni dagli interlocutori, ai sensi dell'art. 351 c.p.p. non venendo in rilievo in tale ipotesi né le disposizioni sulle intercettazioni telefoniche né la tutela costituzionale della segretezza delle comunicazioni di cui all'art. 15 Cost., trattandosi di attività che rientra nelle funzioni proprie della polizia giudiziaria, volta ad assicurare le fonti di prova e raccogliere ogni elemento utile per la ricostruzione del fatto e l'individuazione del colpevole".

2. Digital evidence: cenni tecnici di base

Le fonti d'informazione sono la base delle attività investigative. Se, da un lato, nel mondo cosiddetto "analogico", un colpevole può inconsapevolmente lasciare impronte su oggetti o elementi organici contenenti tracce di DNA, anche nel mondo digitale le attività svolte dal frodatore o dal criminale informatico lasciano (o possono lasciare) una traccia sui sistemi.

Raccogliere ed analizzare tali informazioni è parte fondamentale delle attività di Digital forensics & Digital Investigation. Tali informazioni, infatti, potrebbero costituire una "fonte di prova", ossia permettere (o fornire elementi utili a permettere) la ricostruzione della dinamica attraverso la quale è stato perpetrato l'illecito.

Per questo motivo, è opportuno eseguire una prima distinzione tra **evidenze digitali ed evidenze non digitali**, poiché entrambe possono costituire elementi fondamentali per l'esecuzione di un'attività di digital forensics.

Le evidenze digitali sono quelle fonti di prova memorizzate in strumenti informatici, come le postazioni di lavoro degli utenti, i server aziendali, il Cloud o altri sistemi c.d. informatici/telematici. Questo tipo di evidenze sono caratterizzate da una "carenza di fisicità" che porta ad una maggiore facilità di modifica accidentale durante la fase di acquisizione delle stesse. Si consideri, ad esempio, l'atto di apertura si un documento di testo, necessario alle indagini. Tale apertura può essere sufficiente per modificarne alcune caratteristiche, spesso utili in casi dove la linea del tempo ha una valenza di interesse per le indagini, come ad esempio in un alibi. Affinché il dato sia mantenuto intatto è, pertanto, necessario agire con la massima attenzione e attraverso l'ausilio di strumenti appositi.

Le evidenze non digitali sono tutte quelle fonti di prova che non sono memorizzate in dispositivi informatici come, ad esempio, la stampa di un bollettino falso, del denaro contraffatto, ecc.

Va precisato che questa trattazione esula dal voler indicare metodologie per l'acquisizione di evidenze non digitali, ad esclusione di quelle contenenti dati o informazioni in formato digitale (si pensi ad una fotocopiatrice, ad una stampante con memoria interna, oltre che ad un hard disk, ecc.). In ogni caso, come meglio compendiato successivamente, è comunque richiesto che venga rispettato il **massimo rigore metodologico**: sarà pertanto necessario produrre un verbale (o documentazione similare), oltre che realizzare la catena di custodia secondo quanto illustrato nel tratto a venire.

3. Classificazione delle "evidenze digitali"

Le evidenze digitali possono rappresentare:

• il "**corpo di reato**", come informazioni confidenziali trafugate (o copiate illegalmente), o materiale illegale;
• **informazioni** che consentono la tracciatura delle attività compiute sui sistemi (anche per definire un alibi c.d. informatico).

Un aspetto parzialmente collegato al precedente è rappresentato dalle "posizioni" in cui le evidenze digitali sono reperibili.
La ricerca di informazioni dovrà infatti estendersi a:

• documenti e log [7] sui sistemi coinvolti (computer, periferiche, ecc.);
• log degli elementi infrastrutturali della rete.

Per quanto concerne i log files, questi ultimi forniscono solitamente informazioni circostanziali o aggiuntive, che permettono la tracciatura di eventi. Raramente ad essi hanno accesso i soggetti coinvolti, a meno di illeciti compiuti da attori con elevate competenze tecniche. Ad esempio, le informazioni di logging del sistema operativo e delle applicazioni, pur essendo in molti casi memorizzate sulla postazione di lavoro, non sono accessibili da soggetti diversi dagli amministratori della macchina, o che pur essendolo non ne conoscono la localizzazione.

4. Dati e log sui sistemi coinvolti: cenni

La raccolta diretta delle informazioni sui sistemi coinvolti, solitamente costituiti da personal computer, server o periferiche ad essi direttamente connesse (acceduti o utilizzati dai responsabili dell'illecito), sarà oggetto precipuo dei successivi capitoli.
Sin da ora, tuttavia, è opportuno sottolineare che un elemento chiave per la scelta del metodo di raccolta delle informazioni su tali sistemi, che potenzialmente ospitano dati di interesse per l'indagine nel momento dell'attività investigativa, dipende dallo stato in cui il dispositivo viene rinvenuto (tendenzialmente: operativo, in stand-by e spento/scollegato).

---

[7] I c.d. log files o file di log (o, ancora più sinteticamente, Log) sono informazioni prodotte dall'utilizzo delle infrastrutture ICT e costituiscono le c.d. "tracce informatiche" che rappresentano un'eccellente fonte di informazione per la gestione dei sistemi ICT oltre che elementi investigativi.

L'unico stato in cui si può avere un'accettabile probabilità che i **dati** rimangano **immutati nel corso del tempo** (ed in particolare durante lo svolgimento delle attività preliminari all'attuazione di tutte le contromisure che permettano l'acquisizione "sicura" della fonte di prova) è che il dispositivo sia **spento o scollegato**. Si pensi, ad esempio, ad una chiave USB che, tendenzialmente, mantiene i propri dati intatti finché non viene collegata ad un dispositivo in grado di accedere al contenuto di questa.

Al contrario, se l'investigatore dovesse imbattersi in sistemi attivi o in standby dovrà procedere tenendo conto che ogni operazione effettuata sul sistema potrebbe portare alla **compromissione dei dati**, ma potrebbe anche favorire l'identificazione di importanti informazioni che altrimenti non potrebbero essere rilevate (i processi attivi in quel determinato momento, i contenuti della memoria RAM, lo stato delle schede di rete, le tabelle di routing, ecc.). Nelle parti successive si affronteranno le tematiche afferenti ai possibili approcci ad un sistema che non si presenta spento.

5. Log e informazioni degli elementi infrastrutturali della rete o di sistemi di supporto: cenni

Come anticipato precedentemente, oltre alla ricerca di elementi probatori negli strumenti di memorizzazione dei soggetti coinvolti, molte volte risultano determinanti le **informazioni di tracciatura memorizzate dai sistemi infrastrutturali** (in particolar modo nella c.d. network forensics aziendale). Tipicamente, le informazioni di questo tipo sono da ricercarsi su elementi quali, ad esempio:

- Firewall
- Intrusion Prevention Systems
- Proxy di navigazione
- Domain Controller
- Server di Posta
- Sistemi di Identity Management
- Server Applicativi (SAP, CRM, Custom, ecc.)

Molteplici sono gli elementi tecnologici in grado di produrre tracce e maggiori sono le relative fonti di informazione. Per questo motivo appare di fondamentale importanza scegliere oculatamente le fonti d'informazione da cui estrarre i dati. Se, da un lato, è vero che poche informazioni possono essere insufficienti a delineare il quadro completo o a chiarire l'accaduto, è anche vero che una mole eccessiva di dati può rendere assai complessa l'individuazione delle informazioni utili. Si consideri che molti apparati, tra quelli sopra citati, realiz-

zano log nel formato "Syslog"; questo standard viene anche utilizzato diffusamente per l'implementazione di sistemi di centralizzazione dei log (per uniformare il formato di trasmissione e raccolta delle informazioni), pertanto conoscerne le modalità di funzionamento rappresenta un elemento importante in ambito forense.

6. Le fasi del processo di digital forensics: gli standard internazionali

Il processo di cristallizzazione della fonte di prova è un'attività mirata a congelare i dati contenuti nel sistema in modo da attribuirgli le caratteristiche di protezione richieste, definite anche dalle best practices del settore. Si considerino, ad esempio, le informazioni che sono memorizzate all'interno dei file di log di un server: tali log vengono sovrascritti con una certa periodicità, pertanto è essenziale estrarre le informazioni che possano configurarsi come fonte di prova prima che queste vengano cancellate o modificate.

Al fine di fornire uno standard internazionale, che potesse essere "neutro" rispetto alle singole normative, nel 2012 è stata emessa la ISO 27037:2012, che allo stato dell'arte individua le linee guida per specifiche attività nella gestione delle evidenze digitali. Questo standard fornisce una guida per l'identificazione, raccolta, acquisizione, gestione, protezione e conservazione delle digital evidence.

Lo scopo fondamentale di siffatti standard è promuovere metodi e processi di best practices per l'acquisizione e l'investigazione scientifica delle digital evidence, con l'auspicio che tale standardizzazione porti (eventualmente) all'adozione di approcci simili se non identici a livello internazionale, rendendo più facile il confronto e l'ammissibilità dei risultati di tali indagini anche se eseguite da persone o organizzazioni diverse e potenzialmente in diverse giurisdizioni [8].

Come già detto in più occasioni, uno dei problemi più critici nelle digital forensics è l'acquisizione e la conservazione delle evidenze in modo da garantirne l'integrità. Come per le prove fisiche "convenzionali", è fondamentale che coloro che arrivano per primi o come specialisti sulla scena del crimine (definiti dalla ISO come "Digital Evidence First Responders" e "Digital Evidence Specialists"), possano mantenere la catena di custodia di tutte le evidenze, assicurando che siano raccolte e protette attraverso processi strutturati che siano accettabili per i tribunali. Oltre che fornire "semplicemente" l'integrità, tali processi devo-

[8] Cfr. M.A. BIASIOTTI-M. EPIFANI-F. TURCHI, *Trattamento e scambio della prova digitale, in Europa*, Napoli, 2015.

no garantire che non si possa verificare nulla di negativo. Ciò richiede che venga raggiunto o superato un buon livello di sicurezza delle informazioni.

Prima del rilascio di ISO/IEC 27037, non c'erano standard accettati a livello globale sull'acquisizione delle digital evidence. Come vedremo successivamente, alcune associazioni e forze di polizia hanno sviluppato – in ambito internazionale principalmente – le proprie linee guida e procedure nazionali per l'acquisizione e la protezione delle prove elettroniche. Tuttavia, **ciò può creare problemi quando vengono commessi reati transnazionali**, dal momento che le digital evidence acquisite in un paese potrebbero dover essere presentate davanti a tribunali di un altro. Le prove alterate potrebbero essere state acquisite o protette senza il livello richiesto di sicurezza potrebbero essere giuridicamente inammissibili.

Lo standard fornisce una guida dettagliata sull'identificazione, raccolta e/o acquisizione, etichettatura, conservazione, trasporto e conservazione delle prove elettroniche, in particolare per garantirne l'integrità. Definisce e descrive – inoltre – i processi attraverso i quali le evidenze sono riconosciute e identificate, la documentazione della scena del crimine, la raccolta e la conservazione delle fonti di prova, oltre che la repertazione ed il trasporto.

L'ambito copre i sistemi ed i media IT c.d. "tradizionali" ma anche che i sistemi più "complessi" e specifici quali veicoli, il Cloud computing, ecc. Lo standard è rivolto principalmente ai primi che raggiungono la *scena criminis*.

Oltre alla ISO27037, esistono altri standard internazionali di interesse, emessi negli anni successivi:

a) **ISO / IEC 27041,** che offre una guida sugli aspetti di garanzia della digital forensics, ad es. assicurando che i metodi e gli strumenti appropriati siano utilizzati correttamente.

b) **ISO / IEC 27042**, che indica ciò che accade dopo aver raccolto le digital evidence, ovvero le attività di analisi ed interpretazione.

c) **ISO / IEC 27043**, sulle più ampie attività di indagine sugli incidenti informatici, in cui di solito si verificano le analisi forensi.

d) **ISO / IEC 27050** (in 4 parti), che riguarda l'e-discovery.

Questo standard è per alcune parti ancora in "draft".

Riprendendo gli standard citati e aggiungendo alcuni passaggi non previsti (ma, ad avviso di chi scrive, analogamente importanti), si può dire che il processo di digital forensics deve prevedere l'esecuzione delle seguenti macro-attività:

a) Riconoscimento e identificazione della fonte di prova.

b) Acquisizione del dato (o del sistema).

c) Conservazione e protezione del dato (o del sistema), trasversale rispetto a tutte le successive fasi.

d) Analisi forense.

e) Valutazione dei risultati estratti dall'analisi (sotto il profilo tecnico, giuridico ed investigativo).

f) Presentazione dei risultati (al titolare delle indagini, al giudice o al committente – anche azienda – in caso di attività stragiudiziale).

Tali macro-attività rappresentano il ciclo di vita del dato nell'ambito dell'analisi forense dal momento della sua identificazione fino alla chiusura delle attività. In particolare, le azioni più delicate di cristallizzazione sono quelle relative alle lett. a), b) e c). Dalla d) alla f), invece, le azioni sono meno delicate in quanto si lavora su una copia forense del dato in parola. Comunque, le attività devono essere sempre affiancate dalla redazione della documentazione sulla catena di custodia e di appositi verbali nei quali vengono riportate dettagliatamente tutte le attività svolte.

Per quanto concerne l'identificazione del sistema informatico o telematico, appare utile definire il "ruolo" dello stesso all'interno delle attività investigative e quindi di digital forensics.

Possiamo identificare, a titolo esemplificativo, i seguenti scenari:

a) Parte "attiva" dell'azione illecita (es.: un sistema informatico dal quale l'attaccante esegue un accesso abusivo a sistema informatico e/o telematico).

b) "Obiettivo" delle azioni illecite (es.: un sistema informatico oggetto di un accesso abusivo).

c) Mero contenitore delle informazioni digitali (es.: un file con *ivi* indicate tariffe ed acquirenti di droga).

d) Sistema per comunicare (es.: posta elettronica o chat).

e) Sistema di pagamento per attività illecita (sia come "attaccante" che come vittima, ad esempio home banking, carte di credito/paypal, bitcoin).

f) Alibi informatico.

7. Digital forensics: le classificazioni tipiche

Esistono differenti approcci tecnici all'analisi dei sistemi informatici in seguito all'identificazione di un possibile illecito.

Nell'esame dei dati informatici utili all'attività ispettiva, occorre differenziare due tipologie di approcci in funzione dello stato di funzionamento dei dispositivi che si intende acquisire nel corso delle attività.

In particolare, secondo lo standard ISO/IEC 27042 – Guidelines for the analysis and interpretation of digital evidence, trattasi di:

Analisi *post-mortem* (definita anche static analysis): ci si riferisce ad una

analisi effettuata a macchina spenta, eseguita dopo la consumazione di un illecito. Questo tipo di attività è la più frequente nelle azioni di polizia giudiziaria, quando ad esempio si sequestra un hard disk o altra memoria da analizzare, successivamente, in laboratorio (o presso un consulente tecnico).

Live Forensics Analisys: comprende tecniche di analisi su sistemi attivi, sviluppate negli ultimi anni; nel caso ad esempio di flagranza di reato per accesso abusivo a sistemi informatici, spesso non vi sono molte tracce sugli hard disk ma le informazioni possono essere allocate sulla memoria RAM (quella temporanea). Tali dati si perderebbero spegnendo il dispositivo con le modalità note nel settore [9]; inoltre, spesso i dispositivi di memoria sono protetti da meccanismi di cifratura, ed anche le chiavi sono contenute nella memoria temporanea.

Un'altra tipologia di (sotto)classificazione della digital forensics [10], dipendente dal campo di applicazione, può essere la seguente:

Disk Forensics: è una specifica attività legata all'estrazione di informazioni dagli hard disk (e più in generale alle memorie di massa) dei sistemi previa generazione di immagini forensi, su cui effettuare le relative analisi.

Memory Forensics: si riferisce al recupero dell'informazione contenuta nella memoria RAM di un computer, caratterizzata da una forte volatilità (generalmente non sopravvive allo spegnimento) [11]. Tale attività si interseca con la Disk Forensics precedentemente citata, ove si consideri l'analisi dello SWAP Space.

Network Forensics: il termine si riferisce all'analisi di sistemi di rete, al fine di determinare elementi probatori inerenti ad un determinato caso investigativo.

---

[9] La modalità più nota è quella della disconnessione "bruta" della corrente elettrica (per la maggior parte dei sistemi), preferibilmente staccando il cavo dal computer e non dalla presa del muro (per evitare che un sistema "tampone" possa consentire al sistema di restare accesso comunque). *Contra*, AA.VV., *Diritto penale dell'informatica. Dai computer crimes alla digital forensics*, a cura di D. D'AGOSTINI, Forlì, 2007, 173 ss., dove secondo gli autori tale approccio tecnico potrebbe determinare la distruzione di prove informatiche o perdita dei dati per i proprietari del sistema. Per la descrizione di un caso pratico dove la polizia giudiziaria aveva operato lo spegnimento di un computer acceso sulla scena del crimine, si segnala G. NICOSIA-D.E. CACCAVELLA, *Indagini della difesa e alibi informatico: utilizzo di nuove metodiche investigative, problemi applicativi ed introduzione nel giudizio*, in *Dir. Internet*, 2007, 5, 525.

[10] In questa classificazione non si fa riferimento alla mobile forensics e all'analisi di sistemi embedded.

[11] Durante il 2008, l'Università di Princeton, in California, ha effettuato uno studio dimostrando l'insicurezza di un computer spento. Si è scoperto che le cariche dei moduli della RAM si scaricano lentamente dopo che il viene spento. Qui è disponibile la documentazione ed un video dimostrativo *http://citp.princeton.edu/memory/*. Lo studio, anche se di pregio per quanto concerne i risultati, non può definirsi una pratica comune o best practice.