Parte prima

L'informatica forense e la vehicle forensics

SOMMARIO: 1. L'informatica forense e le sue declinazioni. – 2. Le *best practice* e gli standard internazionali. – 3. Le prime fasi del trattamento del dato digitale. – 4. L'analisi del dato digitale.

1. L'informatica forense e le sue declinazioni

La prima definizione in letteratura italiana sull'informatica forense è ad opera di Maioli[1] che la definisce come «la disciplina che studia l'insieme delle attività che sono rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova». In un'accezione più ampia, l'informatica forense – che negli ambienti anglosassoni è nota come *digital forensics* – si occupi del dato digitale da utilizzare per fini probatori in qualunque ambito del diritto, pertanto gli scopi dell'informatica forense sono l'identificazione, la raccolta, la conservazione, l'acquisizione, l'analisi, la valutazione e la presentazione dei dati digitali memorizzati in qualsiasi tipologia di supporto.

A seconda delle peculiarità del sistema informatico o del dispositivo di memorizzazioni di dati digitali da trattare, l'informatica forense può essere meglio classificata in varie specializzazioni. Ciascuna di queste aree si differenzia dalle altre principalmente per due aspetti strettamente correlati tra loro: la modalità di raccolta e acquisizione della prova digitale può essere più o meno complessa, con una correlata probabilità rischio di alterazione o addirittura distruzione – talvolta controllabile,

---

[1] MAIOLI C., *Dar voce alle prove: elementi di informatica forense*, in *La sicurezza preventiva dell'informazione e della comunicazione* (a cura di P. Pozzi), 2004, pp. 66-75. Per un inquadramento del perimetro della disciplina si veda MAIOLI C., *Questioni di informatica forense*, Aracne, 2015 e BRIGHI R., *Una governance integrata per nuovi modelli dell'informatica forense*, in *I-LEX*, 2017, 11(1), pp. 45-70.

talvolta inevitabile – della prova, che ha significative ricadute sulle procedure previste all'interno dell'ordinamento.

Per raggiungere questi obiettivi occorre innanzitutto individuare le modalità migliori per acquisire i dati digitali senza alterare o modificare il sistema informatico sul quale sono memorizzati, garantendo l'identicità dei dati acquisiti con quelli originali in modo da poterli esaminare senza alterarli.

La *disk forensics* è la prima e principale branca dell'informatica forense, tanto che spesso si utilizza anche il termine *computer forensics* per riferirsi alla scienza forense informatica. La disk forensics si occupa dell'analisi di dispositivi di memorizzazione di dati digitali, cioè di supporti informatici in grado di conservare dati digitali per lungo termine (ad esempio hard disk, solid state disk, chiavette USB, DVD…).

Tuttavia, poiché i sistemi informatici raramente lavorano in maniera isolata ma, disponendo di una connessione di rete, comunicano con altri sistemi, l'esame di un singolo dispositivo può rivelarsi spesso insufficiente se non inutile. Ne consegue che l'analisi forense risente dello sviluppo di tecnologie basate su reti di computer: il focus di chi ricerca ed esamina dati digitali si estende anche a sistemi remoti e ai dati in transito. Interviene quindi la *network forensics* che ha come oggetto di indagine le tecniche di trattamento del dato digitale nel caso di dati in transito e di dati distribuiti su più sistemi[2]. La terza principale specializzazione dell'informatica forense è la mobile forensics, nella quale oggetto di indagine è il dispositivo mobile e i dati e dispositivi ad esso associati: si parla quindi di *mobile handset forensics* (o *cell phone forensics*) quando l'oggetto analizzato è il contenuto del dispositivo mobile (smartphone, tablet, cellulare, ecc.) *SIM card forensics*, quando l'oggetto analizzato è il contenuto della scheda SIM, *memory card forensics* quando l'oggetto analizzato tramite tecniche di disk forensics è una scheda di memoria che potrebbe essere impiegata per estendere le capacità di memoria del dispositivo di memoria, c*ellsite forensics* quando l'oggetto di indagine sono i tabulati telefonici che contengono le tracce lasciate dai dispositivi mobili lungo la rete, consentendo di geolocalizzare un dispositivo nel tempo e nello spazio[3].

---

[2] Sul punto sia consentito il rimando a FERRAZZANO M., *Aspetti metodologici, giuridici e tecnici nel trattamento di reperti informatici nei casi di pedopornografia*, Aracne, 2018.

[3] Sul punto si vedano FERRAZZANO M., REALE P., *Una proposta di progetto open source per l'analisi di tabulati telefonici in risposta a problematiche ed errori ricor-*

Nell'intersezione tra disk forensics, network forensics e mobile forensics si colloca la *cloud forensics*[4]: la possibilità di erogare servizi che gestiscono parte o la totalità dei dati all'esterno sui sistemi del *cloud service provider* rappresenta per l'informatico forense un'importante opportunità di recupero di dati anche in casi di difficile reperimento, distruzione o mancata collaborazione da parte del titolare[5]. Da ognuno di questi ambiti possono essere recuperati dati di varia tipologia. Nel caso di materiali multimediali (audio, immagini, video) è possibile lavorare per migliorare la qualità per cercare di recuperare informazioni altrimenti difficilmente visibili.

Di recente lo sviluppo tecnologico sui veicoli richiede lo sviluppo di competenze, metodologie e tecniche per la raccolta e l'analisi di dati che rientrano nel novero delle attività di vehicle forensics.

I sistemi che non ricadono in nessuna delle collocazioni precedentemente descritte rientrano sotto l'ambito dell'embedded forensics: in questo caso ci si occupa di affrontare l'analisi forense dei sistemi digitali non classificabili nelle precedenti categorie. Sono infatti sempre più numerosi gli strumenti digitali specializzati che possono contenere tracce utili ai fini di un'indagine[6]: si pensi ad esempio a consolle di videogame (PlayStation, Xbox, ecc.), sistemi di rilevamento di intrusione e così via.

---

renti, in *Informatica e diritto*, 24(1-2), 2015, pp. 373-389; JANSEN W., AYERS R., *Guidelines on Cell Phone Forensics*, NIST, 2007, online su *http://www.4law.co.il/cell1.pdf*; HOY J., *Forensic radio survey techniques for cell site analysis*, Wiley, 2015.

[4] Sul punto si veda, in particolare, FEDERICI C., *Nuovi orizzonti per l'acquisizione remota di Personal Cloud Storage*, in *Questioni di Informatica forense* (a cura di C. Maioli), Aracne, Roma, 2015.

[5] La possibilità di acquisire dati da soggetti terzi che forniscono servizi in cloud va valutata sulla base della possibilità di avvalersi di idonei strumenti giuridici.

[6] Gli esempi sono molteplici. Tra tutti si vedano: GAMMAROTA A., CACCAVELLA D., *L'informatica forense per l'E-Health*, in *Strumenti, diritti, regole e nuove relazioni di cura. Il paziente europeo protagonista nell'eHealth* (a cura di C. Faralli, R. Brighi, M. Martoni), Giappichelli, 2015, pp. 205-220; BARDARI U., *L'esperimento giudiziale su posizionamento GPS e scatole nere per automobili*, in *Informatica giuridica e informatica forense al servizio della società della conoscenza* (a cura di R. Brighi, M. Palmirani, M.E. Sanchéz), Aracne, 2018, pp. 241-254.

2. Le *best practice* e gli standard internazionali

Il trattamento della prova digitale non è mai stato oggetto di approfondimento tecnico da parte del legislatore che ha avuto giustamente maggiore interesse a focalizzarsi sul risultato che deve essere ottenuto piuttosto che sul metodo da seguire[7]: in particolare nel settore informatico la definizione di procedure e tecniche di trattamento all'interno di norme giuridiche avrebbe rappresentato una zavorra più che una garanzia in considerazione della differenza di velocità tra il processo legislativo e l'evoluzione tecnologica. A fronte di norme attente a fornire garanzie alle parti e adeguati risultati, le scienze forensi si basano su protocolli scientifici definiti da organismi in grado di garantire maggiore velocità – oltre che competenza tecnica – nella definizione e nell'aggiornamento delle regole del gioco. Per quanto attiene l'informatica forense fino all'ottobre 2012 le metodologie erano definite in alcune best practice del settore, volte a delineare i paradigmi dell'agire tecnico in ambito forense, attraverso una metodologia di base che miri:

- all'acquisizione della prova senza alterare o danneggiare il dispositivo originale;
- all'autenticazione del reperto e dell'immagine acquisita;
- a garantire la ripetibilità dell'accertamento;
- a un'analisi senza modificazione dei dati originari;
- alla massima imparzialità nell'agire tecnico.

Da qualche anno vari standard promossi dall'ISO e da IEC[8] rappresentano le norme tecniche di riferimento anche per garantire un lin-

---

[7] GAMMAROTA A., *Informatica forense e processo penale: la prova digitale tra innovazione normativa e incertezze giurisprudenziali*, 2016, online su *http://amsdottorato.unibo.it/7723/*.

[8] ISO (Organizzazione Internazionale per la Standardizzazione) e IEC (Commissione Elettrotecnica Internazionale) formano il sistema specializzato per la standardizzazione a livello mondiale. Gli enti nazionali che sono membri dell'ISO e dell'IEC partecipano allo sviluppo degli standard internazionali attraverso commissioni tecniche istituite dalle rispettive organizzazioni per occuparsi di campi specifici dell'attività tecnica. Le commissioni tecniche di ISO e IEC collaborano in ambiti di mutuo interesse. Prendono parte ai lavori anche altre organizzazioni internazionali, governative e non governative, in collaborazione con ISO e IEC. Il compito principale della Commissione tecnica congiunta è di redigere gli standard internazionali i cui progetti, adottati dalla Commissione tecnica congiunta, vengono fatti circolare fra gli organismi internazionali per il voto. La pubblicazione a livello di

guaggio comune internazionale: in particolare lo standard ISO/IEC 27037:2012, emesso in versione definitiva il 15 ottobre 2012 relativamente a linee guida per identificazione, raccolta, acquisizione e conservazioni delle prove digitali. Si tratta di un documento che nella sua definizione richiama altri standard ISO/IEC[9] e suggerisce linee guida che si possono certamente considerare come il protocollo operativo di riferimento nel settore dell'informatica forense per le fasi di identificazione, raccolta, acquisizione e conservazione delle prove digitali necessarie in una qualsiasi indagine che necessita di mantenere l'integrità delle prove digitali[10].

Lo standard ha lo scopo di offrire una guida ai soggetti responsabili dell'identificazione, raccolta, acquisizione e conservazione delle potenziali prove digitali:

- il *Digital Evidence First Responder* (DEFR), soggetto autorizzato, preparato e qualificato per intervenire per primo sulla scena di un incidente raccogliendo ed acquisendo le prove digitali con la responsabilità della loro gestione;
- il *Digital Evidence Specialist* (DES), soggetto che svolge le mansioni di un DEFR ed ha conoscenze specialistiche, capacità ed abilità nella gestione una grande varietà di questioni tecniche;
- specialisti di incident response;
- manager dei laboratori di informatica forense.

Il documento prevede che i soggetti responsabili gestiscano le potenziali prove digitali con metodologie che siano adeguate su scala mondiale, con l'obiettivo di facilitare l'investigazione riguardo i dispositivi e le prove digitali in maniera sistematica e imparziale, preservandone al contempo l'integrità e l'autenticità. Lo standard intende altresì offrire informazioni ai soggetti responsabili a livello decisionale che

---

standard internazionale richiede l'approvazione di almeno il 75% degli enti nazionali esprimenti un voto.

[9] ISO/TR 15801 – Document management – Information stored electronically – Recommendations for trustworthiness and reliability. ISOI/IEC 17020 – Conformity assessment – Requirements for the operation of various types of bodies performing inspection. ISO/IEC 17025:2005 – General requirements for the competence of testing and calibration laboratories. ISO/IEC 27000 – Information technology – Security techniques – Information security management systems – Overview and vocabulary.

[10] Sul punto cfr. BRIGHI R., MAIOLI C., *Un cambio di paradigma nelle scienze forensi. Dall'armonizzazione tecnico-giuridica a una nuova cornice epistemologia*, in *Informatica e diritto*, 24(1-2), 2016, pp. 217-234.

hanno l'esigenza di determinare l'affidabilità delle prove digitali; lo standard è applicabile alle organizzazioni che hanno necessità di proteggere, analizzare e presentare le potenziali prove digitali, dove con questa dizione si intendono i dati che possono essere ricavati da diversi tipi di dispositivi digitali, dispositivi di rete, database e quant'altro purché siano già in formato digitale[11].

A causa della fragilità delle potenziali prove digitali, è necessario applicare una metodologia adeguata ad assicurare la loro integrità e autenticità: lo standard non si occupa pertanto di aspetti legali, delle procedure disciplinari e delle altre azioni relative alla gestione delle potenziali prove digitali che siano estranee allo scopo di identificazione, raccolta, acquisizione e conservazione.

Nella sua applicazione comunque gli operatori devono tener conto dei vincoli legali del paese nel quale si interviene con la prospettiva di semplificare lo scambio fra giurisdizioni delle potenziali prove digitali. Allo scopo di mantenere l'integrità delle prove digitali, gli operatori sono tenuti ad adattare le procedure descritte in ottemperanza ai requisiti legali delle prove previsti dalla giurisdizione specifica.

Lo standard ISO/IEC 27037:2012 integra gli standard ISO/IEC 27001[12] e ISO/IEC 27002[13] e i particolari i requisiti di controllo riguardanti l'acquisizione delle potenziali prove digitali offrendo un ulteriore indirizzo applicativo, oltre a trovare applicazione in contesti indipendenti dai due standard citati.

Nonostante tali introduzioni, numerosi operatori del settore (magistrati, avvocati, operatori di polizia giudiziaria, ma anche sedicenti "consulenti tecnici") non sono adeguatamente preparati o aggiornati su queste tematiche[14], con la conseguenza che talvolta si finisce per danneggiare la prova informatica o ignorarla.

---

[11] Documenti analogici convertiti in formato digitale non rientrano nei campi di applicazione dello standard.

[12] ISO/IEC 27001:2013 – ISO/IEC 27001 – Information security management.

[13] ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls.

[14] ZICCARDI G., *Scienze forensi e tecnologie informatiche: la computer and network forensics,* in *Informatica e diritto*, 25(2), 2006, pp. 103-125.