LA DIGITAL FORENSICS NEL PROCESSO PENALE

Quadro normativo, giurisprudenza, diritto di difesa e aspetti di cyber security

Francesco Lazzini, esperto in scienze forensi, informatica giuridica, nuove tecnologie e diritto dell'informatica

WHITEPAPER 11/2022

ICT Security MAGAZINE

INDICE

ICT Security MAGAZINE

CYBER CRIME CONFERENCE 2023

Iscriviti alla newsletter di **ICT Security Magazine** per conoscere le prossime date, l'agenda e per partecipare alla **11ª Edizione della Cyber Crime Conference**

ICT SECURITY MAGAZINE

1° rivista italiana di sicurezza informatica, attiva da oltre 20 anni, dedicata in forma esclusiva alla cyber security e alla business continuity, si pone l'obiettivo di coinvolgere i più importanti attori del settore, aziende e istituzioni pubbliche, per la diffusione degli elementi conoscitivi legati a tutti gli aspetti della information security.

ABOUT THE AUTHOR

Francesco Lazzini

Esperto in informatica giuridica, nuove tecnologie e diritto dell'informatica

Laureato in giurisprudenza con successivo conseguimento dei master in Scienze Forensi (Criminologia-Investigazione-Security-Intelligence) e in Informatica giuridica, nuove tecnologie e diritto dell'informatica. Attività di studio post-universitario focalizzata in materia di indagini con l'utilizzo del captatore informatico e digital forensics.

Introduzione

Lo sviluppo tecnologico degli ultimi decenni ha determinato rilevanti effetti sulla vita dei singoli e della società tutta. In particolare, l'avvento di Internet e il conseguente avanzamento dell'informatizzazione hanno prodotto un balzo in avanti senza precedenti in termini di progresso scientifico, introducendo il concetto di "era digitale", che va di pari passo con quello di rivoluzione digitale[1]/ informatica e, più in generale, di "società informatizzata"[2]. Concetti a loro volta strettamente correlati a quello di "libertà informatica", inteso come diritto costituzionale all'accesso a Internet[3].

Tali cambiamenti, uniti all'inarrestabile progredire delle nuove tecnologie che ne derivano e velocizzati dall'attuale fase pandemica, stanno impattando in maniera considerevole in quasi tutti i settori. Basti pensare a come siano radicalmente cambiati il lavoro alla luce dello *smart working*, l'economia con la *blockchain* e le criptovalute o l'istruzione con la didattica a distanza; senza dimenticare l'ambito sanitario o dei trasporti, la socialità sempre più legata ai *social network* e via discorrendo.

Tra i mondi più colpiti da questa innovazione rientrano a pieno titolo anche il diritto – ivi compreso il diritto processuale – e le scienze forensi. Ciò soprattutto negli ambiti specifici dell'investigazione e della criminalistica, dove i nuovi strumenti digitali vengono utilizzati in maniera ormai consistente, spesso arrivando a costituire elementi essenziali per le indagini su fatti di reato o per la ricerca, acquisizione e repertazione delle relative

[1] Per rivoluzione digitale si intende *"La grande trasformazione della società conseguente all'adozione di strumenti digitali di calcolo automatico"*, da https://www.treccani.it/enciclopedia/rivoluzione-digitale_%28altro%29/

[2] Sul concetto di società informatizzata si veda V. FROSINI, "Implicazioni sociali dei vantaggi e degli svantaggi della rivoluzione informatica", in "Informatica e diritto", Vol. XIII, Fasc. 3, 1987, p. 8, dove si legge: *"The information society is, therefore, a society wich gains informations through information retrieval systems or, in other words, through informatics and telematics".*

[3] Sul Sul punto si veda T. E. FROSINI, *"Il diritto costituzionale di accesso ad Internet"*, in *"AIC Associazione Italiana dei Costituzionalisti"*, n. 1 del 2011, data di pubblicazione 15/12/2010.

prove, soprattutto quando rinvenute all'interno di sistemi informatici (siti web, archivi cloud etc.) o dispositivi elettronici (computer, smartphone, tablet, etc.).

È proprio in tale contesto che si pone la *digital forensics*, talvolta definita anche informatica forense, intesa come *«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»* mediante il ricorso a tecniche volte a garantirne *«l'integrità, "l'autenticità" e la disponibilità»*[4].

Più semplicemente, la locuzione d*igital forensics* fa riferimento alle tecniche di estrazione (o meglio acquisizione) da dispositivi e sistemi informatici dei dati di interesse per il procedimento penale (cd. *Digital evidence*) volte a impedirne l'alterazione e dunque a preservarne la genuinità, fondamentale per il loro utilizzo in sede processuale.

La crescente importanza della *digital forensics* è d'immediata percezione se si considera che tali dispositivi e sistemi sono utilizzati da milioni di persone nella loro vita di tutti i giorni e, sempre più spesso, vengono usati anche per commettere crimini – dai reati contro il patrimonio al terrorismo nella sua moderna declinazione[5] – nonché, talvolta, per l'archiviazione di elementi connessi al reato: si pensi a video o fotografie prodotti durante l'azione criminosa oppure successivamente caricati sul dispositivo, o ancora a comunicazioni via chat da cui emergano "confessioni" o pianificazioni dell'attività criminosa.

Di conseguenza l'analisi di supporti informatici è ormai diventata una fase imprescindibile nell'attività investigativa e, comunque, un irrinunciabile ausilio per gli inquirenti.

[4] G. COSTABILE, *"Digital forensics & digital investigation: classificazione, tecniche e linee guida nazionali ed internazionali"*, in *"Cyber forensics e indagini digitali Manuale tecnico-giuridico e casi pratici"*, a cura di S. ATERNO, F. CAJANI, G. COSTABILE e D. CURTOTTI, G. Giappichelli Editore, Pioltello (MI), 2021, p. 1.

[5] Per fare un esempio, tra gli altri, si consideri la strage di matrice terroristica di San Bernardino, consumatasi nell'omonima cittadina della California nel 2015, e la successiva controversia giudiziaria avutasi tra l'F.B.I. e la Apple Inc. per l'accesso ai dati contenuti sullo smartphone, protetto da password, di uno dei terroristi. Per un approfondimento si veda M. TORRE, *"Sull'obbligo per il privato di collaborare ad attività di digital forensics – "Il caso Apple F.B.I.""*, In *"Trattato di diritto penale – Cybercrime"*, a cura di A. CADOPPI, S. CANESTRARI, A. MANNA e M. PAPA, UTET Giuridica, Vicenza, 2019, pp.1676 e ss.

Tuttavia, se non vi sono dubbi riguardo all'utilità della *digital forensics*, non ve ne sono neanche circa le problematicità che tale strumento può portare con sé.

Oltreché alla potenziale compressione del diritto alla privacy ci si riferisce ai possibili pregiudizi per il diritto costituzionale alla difesa che, in assenza di opportuni accorgimenti, rischia di scivolare pericolosamente in secondo piano; anche in considerazione dei consolidati orientamenti giurisprudenziali che vedono la prova scientifica – entro la quale va collocata anche la digital evidence – come "prova regina", capace di determinare l'esito del giudizio senza necessità di ulteriori elementi a supporto.

Va ricordato che, stante la loro classificazione come "atti ripetibili", nella maggior parte dei casi tali operazioni si svolgono in assenza di contraddittorio, permettendo all'indagato di contestare l'operato degli inquirenti solo in un momento successivo. L'analisi e l'acquisizione di materiale da dispositivi elettronici e la successiva catena di custodia dei dati repertati, inoltre, si presentano come attività particolarmente delicate attesa la fragilità che caratterizza questa tipologia di prova.

Il tutto appare ancora più problematico se si considera che oggi non esiste, nell'ordinamento italiano, una disciplina dettagliata in tema di *digital forensics*: al riguardo si fa esclusivamente rinvio alle *best practices* elaborate a livello internazionale che indicano agli operatori delle linee guida (in ogni caso non obbligatorie) da poter seguire nello svolgimento delle attività.

Ciò premesso è interessante provare ad analizzare, anche alla luce delle più rilevanti sentenze in materia, l'attuale panorama legislativo in cui si colloca la *digital forensics*, evidenziandone i maggiori problemi; a tale scopo si partirà dalle definizioni di *digital evidence* e di prova scientifica per poi esporre come avvenga in concreto l'acquisizione di elementi di prova da supporti informatici e quali siano i rischi correlati, con particolare attenzione alla fase della catena di custodia dei dati repertati. Verranno infine analizzati alcuni casi che consentono di apprezzare in concreto la delicatezza di una disciplina che, se mal interpretata, rischia di compromettere inevitabilmente il diritto di difesa delle persone indagate e – più in generale – l'intera vicenda processuale.

FORUM ICT SECURITY 2023

Iscriviti alla newsletter di **ICT Security Magazine** per conoscere le prossime date, l'agenda e per partecipare alla **21ª Edizione del Forum ICT Security**

Il concetto di digital evidence e la sua classificazione come prova scientifica

Oggetto del processo di *digital forensics* è l'identificazione, la raccolta, l'acquisizione, l'analisi e la valutazione delle *digital evidence*[6].

Più propriamente con la terminologia *digital evidence* – traducibile in italiano con "evidenza digitale"[7], "prova informatica"[8] o "prova elettronica"[9] – si fa riferimento a *«quelle informazioni memorizzate in strumenti informatici, come le postazioni di lavoro degli utenti, i server aziendali, gli apparati mobili, la rete e/o in qualsiasi dispositivo informatico»*[10] o ancora, con maggiore focalizzazione nell'ambito processuale, *«ogni informazione probatoria la cui rilevanza processuale dipende dal contenuto del dato o dalla particolare allocazione su una determinata periferica, oppure dal fatto di essere stato trasmesso secondo modalità informatiche o telematiche»*[11].

[6] Lo schema procedurale citato è quello desumibile dalle linee guida enucleate dalle cd. *best practices*, primi fra tutti gli standard ISO/IEC 27037:2012 (*Information security management systems*), ISO/IEC 27000:2013 (*Guidelines for identification, collection, aquisition and preservation of digital evidence*) e ISO/IEC 27041 (*Guidances on assuring suitability and adequacy of incident investigative method*), sui quali si tornerà in seguito.

[7] M. DANIELE, *"La prova digitale nel processo penale, in Riv. dir. proc., 2011, p. 283, Cfr. M. PITTIRUTI, Digital evidence e procedimento penale"*, G. Giappichelli editore, 2017, p. 7, dove il concetto prova digitale viene enucleato *"facendo leva sull'essenza del dato, frutto di una manipolazione di una manipolazione elettronica di numeri"*.

[8] G. PIERRO, "Introduzione allo studio dei mezzi di ricerca della prova informatica", in Dir. Pen. proc., 2011, p. 1516 ss., come citato in M. PITTIRUTI, op. cit., pp. 7-8.

[9] V. R. KOSTORIS, *"Ricerca e formazione della prova elettronica: qualche considerazione introduttiva"*, in F. RUGGERI e L. PICOTTI, *"Nuove tendenze della giustizia penale di fronte alla criminalità informatica: aspetti sostanziali e processuali"*, Giappichelli, Torino, 2011, p. 179 ss., come citato in M. PITTIRUTI, op. cit., pp. 7-8.

[10] R. MUNEREC, "Digital Forensics Aspetti tecnico-giuridici e operativi su trattamento dei dati digitali", Egaf Edizioni Srl, 2021, p. 80.

[11] L. MARAFIOTI, "Digital evidence e processo penale", in Cass. Pen., 2011, p. 4509

In buona sostanza, pertanto, per *digital evidence* si devono intendere tutti i dati e le informazioni presenti all'interno di sistemi informatici, sia fisici (computer, smartphone, tablet, etc.) sia presenti in rete, che possono avere valore probatorio o indiziario nei confronti di fatti specifici e quindi assurgere a elemento di prova – ed eventualmente a prova – nelle dinamiche del processo penale; e che si distinguono dalle evidenze non digitali, definibili, per esclusione, come *«tutte quelle fonti di prova che non sono memorizzate in dispositivi informatici»*[12].

A titolo esemplificativo possono essere considerate *digital evidence* le immagini, le conversazioni via chat, i file in generale (ivi compresi i file di log) e i documenti memorizzati su supporto informatico, mentre non può essere considerato alla stregua di *digital evidence* tutto ciò che sia esterno a sistemi informatici, sebbene proveniente dai medesimi (si pensi ad esempio ad un documento cartaceo stampato da computer).

Ciò detto si possono cogliere agevolmente le caratteristiche principali che connotano la prova informatica: prima fra tutte l'immaterialità, dovuta alla sua appartenenza alla dimensione digitale, tratto dal quale discendono tutte le altre peculiarità che interessano la *digital evidence* e che si sostanziano nella sua capacità di essere replicata e di trovarsi contemporaneamente nella memoria di più supporti (ubiquità) nonché nella sua fragilità, attesa la facilità di dispersione derivante dalla sua attitudine a subire variazioni, anche spontanee, o alterazioni e ad essere cancellata con estrema semplicità (volatilità del dato digitale).

In particolare l'immaterialità costituisce una caratteristica intrinseca dell'evidenza digitale[13], la quale si manifesta come dato virtuale e intangibile che per essere apprezzato necessita della presenza di un supporto fisico, che tuttavia non può esserne considerato parte integrante. Infatti, l'esistenza della prova informatica prescinde dal dispositivo elettronico su cui si trova memorizzata, da intendersi piuttosto come strumento funzionale alla sua conservazione e lettura. In termini tecnici, dunque, potrebbe dirsi che il dato digitale non è altro che una sequenza numerica espressa in *bit* che per essere rappresentata ha bisogno dell'ausilio di un apposito supporto idoneo alla sua decodifica (computer, etc.).

[12] R. MURENEC, op. cit., p. 80.

[13] Cfr. F. PELUSO e M. FERNANDES DOS SANTOS, *""Battlefield digital forensics": la raccolta della prova informatica negli scenari di guerra", in "IISFA Memberbook 2019-2020 digital forensics"*, a cura di G. COSTABILE, A ATTANASIO e M. IANULARDO, Cap. V (formato kindle), dove l'immaterialità viene definita come «carattere "genetico" dell'evidenza digitale».

L'immaterialità comporta che il dato digitale possa essere replicato in molteplici copie sul medesimo dispositivo oppure possa essere trasferito su altri supporti ed ivi memorizzato, così da potersi trovare all'interno di più dispositivi nello stesso momento. Proprio questa sua capacità, definibile ubiquità del dato digitale[14], sta alla base del processo di digital forensics, volto ad acquisire le evidenze digitali estraendo la cd. copia forense dal dispositivo oggetto di investigazione, mediante la copiatura *bit to bit* o la funzione di *hash*, sulle quali si tornerà in seguito.

Corollario dell'immaterialità della prova informatica è altresì la sua volatilità, presupposta dal *«rischio di alterazione che caratterizza l'ambiente virtuale»*[15].

Difatti il dato informatico, come anticipato, consiste in una sequenza numerica espressa in linguaggio binario (successioni di 0 e 1) che può essere facilmente modificata da parte di qualunque soggetto (o software) che sia in grado di accedere al dispositivo ove si trova il dato in questione. Talune evidenze – si pensi ad esempio alle informazioni contenute nella memoria RAM[16]– possono inoltre essere soggette a modifiche o cancellazioni "spontanee", dal momento che per la loro alterazione è sufficiente che il dispositivo di riferimento venga spento o si spenga in autonomia, ad esempio per l'esaurirsi della batteria o per l'implementazione di aggiornamenti di sistema.

Infine, alterazioni o cancellazioni, seppure non volute, potrebbero essere erroneamente apportate anche dagli stessi inquirenti o da consulenti tecnici o periti non sufficientemente preparati che si trovano a maneggiare il reperto informatico senza le opportune cautele.

Il rischio di distruzione e danneggiamento a cui può andare incontro il dato informatico se non adeguatamente trattato, con la conseguenza della sua inattendibilità processuale, costituisce il cuore delle problematicità che pervadono la materia delle indagini forensi sui

[14] *Ibidem.*

[15] V. G. CALABRO, *"La fragilità della prova informatica: caratteristiche generali e problematiche emergenti", consultabile sul sito: https://www.vincenzocalabro.it/pdf/2008/LaProvaInformatica.pdf.*

[16] Con il termine memoria RAM, acronimo di Random Acces Memory (memoria ad accesso causale), si fa riferimento al tipo di memoria informatica a breve termine funzionale alla memorizzazione dei dati di cui un programma o un'applicazione hanno bisogno per la loro esecuzione. Detta memoria si definisce volatile poiché una volta chiuso il programma le informazioni vengono cancellate.

dispositivi elettronici; il tutto in considerazione del fatto che ad oggi non esiste nel nostro ordinamento una normativa che disponga le modalità da seguire per l'acquisizione e la conservazione delle digital evidence, bensì viene unicamente delle linee guida, non cogenti, che nel tempo hanno messo a punto una serie di modalità operative.
In realtà, per ora il legislatore non si è nemmeno preoccupato di fornire una definizione giuridica di *digital evidence* o di farne menzione all'interno del codice di rito.
Ad ogni modo, essendo la procedura di acquisizione del dato informatico *«connotata da un alto grado di scientificità»*[17] nonché di tecnicità, la maggiore dottrina ricomprende la *digital evidence* all'interno della categoria della prova scientifica, con ciò inteso quel tipo di prova che, partendo da un fatto noto, si avvale di una determinata legge scientifica per risalire ad un fatto non noto da provare[18].
La categorizzazione della prova informatica come prova scientifica impone che questa non possa essere trattata e valutata con i canoni a cui si fa ricorso per altre tipologie di prove: bensì occorre che, sia durante la fase di individuazione e raccolta sia durante i passaggi della successiva catena di custodia, l'evidenza sia maneggiata con tutte le accortezze che si adottano nei confronti di reperti come il DNA, i campioni biologici, le polveri di residuo dello sparo di arma da fuoco, etc.
In particolare, è necessario che le operazioni siano svolte da personale con accreditata competenza tecnica nel settore e che tutto il procedimento sia documentato dettagliatamente nonché condotto nella maniera più imparziale possibile, in modo da non minare l'autenticità della traccia digitale.
Particolari attenzioni devono essere attuate anche dal giudice in sede di valutazione della prova, dovendo egli ripercorrere in maniera critica tutte le fasi che hanno interessato la *digital evidence* al fine di accertare che quest'ultima non sia – o non abbia potuto essere – incorsa in fenomeni di danneggiamento che, anche solo in linea teorica, ne possano avere contaminato la genuinità[19].

[17] V. G. CALABRO, op. cit., Cfr. F. PELUSO e M. FERNANDES DOS SANTOS, op. cit.

[18] https://www.treccani.it/enciclopedia/prova-scientifica_%28Lessico-del-XXI-Secolo%29/.

[19] Affinché la prova scientifica sia soggetta ad inattendibilità processuale non è necessario che abbia subito concretamente un evento di contaminazione, ma, per metterne in dubbio la genuinità, è sufficiente che tale evento, anche solo ipoteticamente, possa essersi verificato.

Il sopralluogo giudiziario nelle indagini sui sistemi informatici

L'acquisizione della *digital evidence* è la fase del processo di *digital forensics*, successiva all'individuazione dell'evidenza informatica, che mira alla sua estrazione, mediante copiatura, dal supporto elettronico e contestuale trasferimento su altro supporto, in uso agli organi inquirenti, ove l'elemento acquisito viene "cristallizzato" e conservato per essere analizzato ai fini del suo eventuale utilizzo in sede dibattimentale.

Sebbene la fase di acquisizione sia da considerarsi il momento essenziale dell'intero procedimento, essa, cronologicamente, si colloca solo a seguito di una serie di operazioni che rientrano nella più ampia fase del sopralluogo giudiziario sulla scena del crimine[20]. Operazioni dalle quali dipende la corretta riuscita di tutta la fase investigativa e che sono finalizzate all'osservazione della *scena criminis* (o presunta tale), all'identificazione delle fonti di prova e alla loro successiva raccolta mediante l'applicazione di tecniche e metodologie atte a preservarne la genuinità.

In caso di ritrovamento di strumenti elettronici all'interno del *locus commissi delicti*, o in generale in caso di indagini su sistemi informatici, tali attività non possono prescindere dalla messa in sicurezza del dispositivo e dalla protezione del suo contenuto digitale in modo

[20] Per una puntuale definizione di sopralluogo giudiziario, inteso come «esame della scena del crimine», si veda D. CURTOTTI, "Rilievi e accertamenti sul locus commissi delicti nelle evoluzioni del codice di procedura penale", in "Manuale delle investigazioni sulla scena del crimine Norme, tecniche, scienze, logica", a cura di D. CURTOTTI e L. SARAVO, G. Giappichelli Editore, Pioltello (MI), 2019, p. 45, dove, rilevata l'assenza della locuzione sopralluogo giudiziario all'interno del codice di rito, l'esame della scena del crimine viene definito come «quel complesso di attività poste in essere dalla polizia giudiziaria, dal consulente tecnico del pubblico ministero e della difesa, aventi natura tecnica e scientifica, esperibili sul locus commissi delicti, sia nell'immediatezza della scoperta del fatto di reato che nell'esecuzione di eventuali successivi accessi, finalizzate ad isolare, descrivere e analizzare lo scenario, nonché ricercare, esaminare e repertare le tracce ivi rinvenute». Tale definizione appare pienamente calzante anche in ambito di sopralluogo su supporti elettronici e sistemi informatici.

da impedirne mutazioni. Attività che inoltre non possono nemmeno prescindere dalla sua analisi esterna e dalla seguente descrizione dello stato di rinvenimento delle componenti hardware[21] (ivi comprese, oltre al corpo del dispositivo in sé, anche eventuali periferiche come chiavette usb, hard-disk, etc.), anche mediante fotografia.

Se la descrizione del dispositivo costituisce un'attività intuibilmente semplice – essendo sufficiente annotare il luogo di ritrovo, eventuali segni di usura o di rottura, se spento, acceso o in *stand-by* etc. – il congelamento dei dati salvati nel dispositivo o nella sua memoria istantanea in talune circostanze potrebbe rivelarsi un'attività delicata e non scevra dal rischio di alterazioni indesiderate, che potrebbero verificarsi anche a seguito delle scelte operative adottate da chi è chiamato ad intervenire.

È appena il caso di precisare che dette scelte variano a seconda del contesto in cui si opera, dei dati che si intende acquisire e delle circostanze che possono presentarsi nel caso concreto (si pensi ad una batteria quasi scarica, ad un computer connesso alla rete Internet, etc.) oppure, infine, variano con riguardo alla tipologia di dispositivo con cui si ha a che fare e sulla scorta del quale cambiano altresì le tecniche di acquisizione.

Deve tenersi conto del fatto, per l'appunto, che le tecniche di *digital forensics* si differenziano a seconda del supporto informatico oggetto di indagine a causa delle caratteristiche proprie di ciascun sistema: pertanto, se l'indagine riguarda un telefono cellulare, uno smartphone o un tablet occorrerà adottare le tecniche della *mobile forensics*, nel caso di un PC quelle della *computer forensics*, o ancora, nel caso in cui l'acquisizione debba avvenire da sito web, la procedura sarà ancora differente dovendosi tenere in considerazione ulteriori variabili, quali ad esempio la possibilità di modifica del sito da parte di altri utenti, che rendono necessaria l'applicazione di un approccio metodologico differente. Le tecniche differiranno anche a seconda del tipo di memoria che contiene le informazioni ritenute di interesse, ponendosi una divergenza operativa tra memorie di massa – come un disco rigido, una pennetta usb o un cd, dvd, floppy disk etc., dove i dati vengono immagazzinati e, in linea generale, restano immutati (c.d. *disk forensics*) – e memoria RAM, dove la facilità di

[21] Per hardware si intendono le «componenti di base, non modificabili, di un apparecchio o di un sistema (alimentatori, componenti circuitali fissi, unità logiche, ecc.)», https://www.treccani.it/vocabolario/hardware/

dispersione dei dati impone attenzioni particolari (c.d. *memory forensics*)[22].

Ad ogni modo, a prescindere da quale sia il supporto con cui gli investigatori hanno a che fare, esistono alcune precauzioni comuni che si rendono opportune ai fini della salvaguardia delle possibili fonti di prova, una volta che queste siano state riconosciute e identificate come tali. Prima di tutto occorre verificare se il dispositivo sia in funzione, in *stand-by* oppure spento. Quest'ultima situazione è quella meno rischiosa, poiché ad apparecchio già spento è molto difficile che si producano modificazioni indesiderate del suo contenuto digitale, che potrà quindi essere estratto anche a distanza di tempo, con l'ovvio accorgimento di assicurarsi che *medio tempore* non vengano effettuate accensioni che non si dovessero rendere necessarie per circostanze particolari. Le attività di estrazione da dispositivo spento sono denominate operazioni *"post-mortem"* e, in genere, rientrano nelle c.d. attività ripetibili ex art. 359 c.p.p.

Viceversa, in base allo stesso principio, quando il dispositivo viene rinvenuto acceso o in stand-by e vi sono ragioni per ritenere che le informazioni di interesse possano essere contenute all'interno della memoria temporanea (RAM), per sua natura estremamente volatile e suscettibile alla cancellazione con lo spegnimento, o sussistano altre circostanze peculiari come la non rimovibilità del supporto dal luogo d'installazione, l'estrazione dovrà avvenire direttamente sul sistema in accensione – salvo, in ogni caso, che condizioni impeditive ne impongano la disattivazione[23] – applicando le c.d. tecniche di *"live forensics"* e *«tenendo conto che ogni operazione effettuata sul sistema potrebbe portare all'alterazione dei dati»*[24].

[22] Altre discipline che rientrano nell'area della digital forensics sono la cloud forensics, per l'analisi e acquisizione da sistemi cloud, la network forensics, avente ad oggetto l'analisi e l'acquisizione da sistemi di rete e il traffico delle comunicazioni che vi transitano, la database forensics, volta ad analizzare ed acquisire quanto è contenuto all'interno di database.

[23] Si pensi ad esempio ad analisi da eseguire su apparecchi dallo spegnimento dei quali potrebbero derivare situazioni di pericolo come sistemi di gestione del traffico aereo o ferroviario, sistemi militari atti alla difesa nazionale come sistemi radar e scudi balistici etc. o macchinari in ambito sanitario.

[24] R. MURENEC, op. cit. p. 123 e, ugualmente, G. COSTABILE, op. cit., p. 13, dove tra gli altri dati istantanei che potrebbero essere compromessi con lo spegnimento vengono indicati a titolo esemplificativo: processi attivi nel momento del rinvenimento, stato schede di rete e tabelle di routing.

L'esecuzione di analisi e acquisizioni di dati in modalità *live forensics* comporta indubbiamente un maggior rischio rispetto alle attività eseguite *post mortem*; con l'ulteriore considerazione che le operazioni condotte su dispositivi accesi andrebbero ricomprese, almeno in linea teorica, tra gli atti irripetibili ex art. 360 c.p.p., producendosi giocoforza in tali casi delle modificazioni dello stato originale del contenuto digitale che, di conseguenza, ai fini dell'attendibilità processuale delle evidenze estratte e a garanzia del diritto di difesa, devono essere annotate e descritte adeguatamente.

Tra i primissimi accorgimenti da apprestare quando si agisce su un dispositivo attivo vi è quello di impedirne l'uso da parte di soggetti non autorizzati e porlo in una situazione di isolamento rispetto a possibili interferenze esterne, in modo da prevenire alterazioni da terzi che potrebbero sfruttare un qualche tipo di collegamento con il *device*, come connessioni internet o *bluetooth*.

L'isolamento può essere realizzato inserendo il congegno all'interno di una c.d. gabbia di Faraday, cioè un contenitore che non permette la penetrazione di segnali elettromagnetici, oppure mediante l'utilizzo di un *jammer*, strumento che inibisce (entro il suo raggio d'azione) la capacità degli apparecchi elettronici di emettere o ricevere segnali e onde radio. In caso di impossibilità d'uso di simili strumentazioni una soluzione valida potrebbe essere anche impostare il dispositivo *offline* attivando la "modalità aereo", qualora presente tra le funzioni del sistema.

Sempre in sede di sopralluogo giudiziario gli organi inquirenti potrebbero ritenere utile l'espletazione di attività preliminari, anche dette "*preview*", volte ad esaminare il contenuto delle apparecchiature rinvenute nel corso di ispezioni o perquisizioni, col fine di valutare se possa effettivamente trattarsi di materiale utile per le indagini oppure di materiale superfluo, potendo così determinarsi di porre sotto sequestro solamente alcuni dispositivi oppure solo le unità di memoria esterna del dispositivo analizzato[25].

[25] G. COSTABILE, op. cit., p. 12, dove in ottica esemplificativa si afferma che una simile modalità operativa potrebbe comportare risultati positivi in caso di indagini sulla pedopornografia online «dove l'identificazione di materiale illecito detenuto con dolo (quindi presente sull'hard disk e non cancellato) può portare al sequestro dei soli hard disk "inerenti", lasciando fuori dal sequestro materiale "neutro" rispetto alle indagine», mentre non sarebbe funzionale «per stabilire un c.d. alibi informatico o dove si rende necessario analizzare anche i file cancellati o di sistema», vista la necessità per queste ultime ipotesi di effettuare il sequestro di tutto il materiale contenente dati.

Giunti a questo punto, in estrema sintesi, è possibile affermare che in caso di rinvenimento di dispositivi elettronici durante le fasi del sopralluogo giudiziario, la polizia giudiziaria o gli altri soggetti chiamati a intervenire sono tenuti ad attuare una serie di operazioni volte ad assicurare la buona riuscita delle successive fasi investigative, che si potrebbero schematizzare come segue:

- messa in sicurezza del dispositivo, anche mediante isolamento da interferenze esterne e comunque impedendone l'uso da parte di soggetti non autorizzati;
- descrizione del dispositivo (anche mediante foto o video), annotazione delle sue particolarità (usura, eventuali componenti rotte, etc.) e stato di rinvenimento (se acceso, in *stand-by* oppure spento);
- se spento non accendere e, se acceso o in *stand-by*, evitarne spegnimenti che non siano necessari;
- annotazione e descrizione di tutti i passaggi del dispositivo e di eventuali analisi preliminari del contenuto.

Una volta concluse queste fasi e trasportato in laboratorio il dispositivo rinvenuto, salvo eventuali necessità che rendano necessario proseguire nel luogo del ritrovamento (o dell'ispezione/perquisizione), si può far seguito al successivo passaggio del processo di *digital forensics*, consistente nell'acquisizione delle *digital evidence* giudicate di interesse.

Appare opportuno precisare che se in linea di principio tali operazioni, in quanto atti investigativi, ricadono nella competenza del Pubblico Ministero e della polizia giudiziaria, non di rado accade che, quando il quantitativo di dati da estrarre è considerevole e non sussiste pericolo di inquinamento del possibile materiale probatorio identificato, tali organi nominino per l'esecuzione delle attività in questione un ausiliario di polizia giudiziaria. Tale figura, che deve essere scelta tra soggetti con comprovata esperienza tecnica nel settore, talvolta può rivestire un ruolo centrale in questa fase investigativa, potendosi rivelare un valido ausilio non solo per la conduzione materiale dell'estrazione dei dati ma anche nella selezione delle informazioni digitali da acquisire.

White Paper “Quaderni di Cyber Intelligence” #1

CYBER INTELLIGENCE

Download gratuito su www.ictsecuritymagazine.com

Le tecniche di acquisizione delle evidenze digitali: copia *bit a bit* e funzione di *hash*

Procedendo secondo una linea cronologica, esaurite le operazioni del sopralluogo giudiziario – ovvero una volta individuate, identificate e raccolte le evidenze digitali – si apre la fase dell'acquisizione del materiale informatico rinvenuto e giudicato di interesse ai fini processuali.

L'acquisizione della evidenza digitale, che insieme ai passaggi della catena di custodia del dato acquisito rappresenta il momento di maggiore criticità del processo di *digital forensics*[26], può essere definita come il momento afferente alla fase di indagine dove viene eseguita l'esfiltrazione controllata della digital evidence dal sistema informatico perquisito/ispezionato e/o sottoposto a sequestro ai fini del suo trasferimento su altro supporto, mediante particolari tecniche di copiatura e con l'utilizzo di strumentazioni tali da garantirne la completa integrità e genuinità.

Si è già accennato, trattando di sopralluogo giudiziario, agli accorgimenti operativi da adottare in caso di rinvenimento di dispositivi attivi, per i quali si dovrà ricorrere alla l*ive forensics analysis* e, in caso di rinvenimento di dispositivi spenti, sottoponibili ad acquisizione post mortem, nonché della differenza di modalità operative a seconda della natura del dispositivo da analizzare. Quale che sia lo stato di rinvenimento o la tipologia di sistema sul quale si agisce, il risultato delle attività di acquisizione non cambia, sostanziandosi in ogni caso nell'ottenimento della memoria da analizzare sotto forma della c.d. copia forense.

Più propriamente la copia forense, anche detta *bit stream image* o copia *bit a bit*, consiste

[26]-Si veda anche S. ATERNO, *"Digital forensics e scena criminis"*, in *"Manuale delle investigazioni sulla scena del crimine Norme, tecniche, scienze, logica"*, come già citato, p. 782, dove la fase di acquisizione del reperto informatico viene descritta come «*la più complessa e delicata in assoluto*».

nella copiatura integrale del contenuto digitale della memoria del sistema inquisito, che si esegue, per l'appunto, trascrivendo su un altro dispositivo ogni singolo *bit* presente al suo interno, compresi gli spazi vuoti tra *files* e gli elementi cancellati (ma non definitivamente eliminati) dal sistema, o loro frammenti[27]. In buona sostanza, quindi, la copia forense è l'identica riproduzione, in perfetta clonazione[28], della memoria oggetto di indagine, che materialmente si utilizzerà per l'effettuazione dei successivi passaggi del procedimento di *digital forensics*.

Se correttamente eseguita e opportunamente documentata, anche mediante videoregistrazione[29], l'acquisizione in copia forense permette di mantenere intatti i dati contenuti nella memoria di origine, consentendo in un secondo momento di poter valutar e l'attendibilità dei dati estratti, anche al fine di verificare che sia avvenuto correttamente il trasferimento nel dispositivo di destinazione.

Sotto un altro aspetto, l'importanza della *bit stream image* si riflette poi nella fase di determinazione cronologica degli eventi, in quanto tale metodo di copiatura permette di mantenere inalterati anche i metadati relativi ai file acquisiti (come data e ora di salvataggio), permettendo di ricostruire con precisione la timeline delle operazioni condotte sul dispositivo originale[30]. Ricostruzione cronologica che, tuttavia, potrebbe risultare inesatta in caso

[27] Per farsi un'idea dell'accuratezza e della fedeltà della copia forense rispetto all'originale basti pensare che tra le parti di memoria che vengono in essa vengono riprodotte si annoverano anche i c.d. *slack space*, ovvero quelle porzioni di memoria occupate da frammenti di file che, anche se cancellati dal sistema, non sono ancora stati completamente sovrascritti da nuovi dati e pertanto in parte ancora insistenti in memoria. In tal modo è possibile recuperare anche quei dati degni di interesse investigativo che il possessore del dispositivo potrebbe aver eliminato in quanto collegati all'evento criminoso.

[28] Per chiarezza, sul punto preme specificare la differenza che nel settore informatico sussiste tra semplice copia di un sistema, concetto diverso da copia forense, e sua clonazione. La mera copia, infatti, consiste in una semplice copiatura che non rispetta il criterio di identicità, come ad esempio un banale copia e incolla di un file. La clonazione, propria della copia forense, riproduce in completa esattezza l'originale.

[29] La documentazione della fase di acquisizione deve essere eseguita nella maniera più accurata possibile. In proposito si veda anche S. ATERNO, op. cit., p. 782, dove, come buona prassi, si indica l'opportunità di utilizzare, durante tale fase, dispositivi in grado di registrare in automatico le operazioni, così da conservarne traccia.

[30] Si pensi all'impatto investigativo e alla centralità processuale che la ricostruzione cronologica degli eventi ottenuta dai riscontri pervenuti dai dispositivi elettronici ha avuto anche in casi giudiziari di grande clamore mediatico.

di applicazione di tecniche di *anti forensics*[31] sul dispositivo sorgente atte a complicare o depistare le indagini, come ad esempio l'utilizzo di programmi di crittografia per cifrare i dati o l'attuazione di stratagemmi volti alla precostituzione del c.d. *alibi informatico*[32].

Dal punto di vista tecnico, la copia forense si ottiene mediante l'uso di particolari strumenti hardware con funzione di *write blocking*[33] che, una volta collegati al sistema contenente i dati da acquisire, permettono la duplicazione dei dati in sicurezza all'interno della memoria di destinazione, oppure usando appositi software di estrazione dati installati sul dispositivo che si adopera per la manovra. È chiaro che nel caso in cui detti strumenti siano difettosi o settati non correttamente, la duplicazione potrebbe presentare delle difformità rispetto alla memoria sorgente, con conseguenti problemi in ordine all'attendibilità delle operazioni. Occorre pertanto che in sede di esecuzione delle operazioni venga specificato con quale strumento si stia procedendo, in modo da poterne verificare – anche a posteriori – l'attendibilità.

Infine, per garantire l'integrità e l'identicità della copia forense e la conformità delle copie che si possono estrarre dalla medesima, è necessario apporvi la firma digitale mediante la c.d. funzione di *hash*.

Una volta ottenuta la copia forense, infatti, è necessario che la stessa non subisca alterazioni, così da mantenerne l'identicità all'originale. Per garantire tale identicità la copia va, per l'appunto, "firmata" mediante il calcolo della funzione di *hash*, che offre la possibilità

[31] Con la locuzione anti forensics s'intendono tutte quelle tecniche poste in essere al fine di ostacolare o complicare l'analisi forense di un dispositivo. M. D. ROGERS definisce l'anti forensics come *"Attempts to negatively affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct"*. La citazione è tratta da G. C. KESSLER, *"Anti-Forensics and the Digital Investigator"*, 2007, dove vengono evidenziate le principali tecniche di antiforensics. Articolo consultabile sul sito https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.258.5244&rep=rep1&type=pdf.

[32] In proposito si veda V. CALABRÒ, G. COSTABILE, S. FRATEPIETRO, M. IANULARDO, G. NICOSIA, "L'alibi informatico: aspetti tecnici e giuridici", consultabile sul sito https://www.vincenzocalabro.it/pdf/2010/AlibiInformatico.pdf.

[33] Per sistema di write blocking si intende un sistema con funzione di blocco di scrittura, denominato appunto write blocker, che impedisce la scrittura sui dati che si acquisiscono, garantendone pertanto integra la genuinità nel passaggio dalla sorgente fino al salvataggio nella memoria del dispositivo di destinazione.

di verificare l'integrità del documento per poterne stabilire la veridicità nelle successive fasi investigative e giudiziali, marchiandolo con un'impronta digitale individualizzante, in grado di dare completa certezza relativamente all'origine del reperto e all'integrità del suo contenuto.

La funzione di *hash* consiste in un calcolo matematico (o meglio un algoritmo) non invertibile, ossia è che opera in una sola direzione, che applicato al documento ne traduce il contenuto – inteso come testo di lunghezza arbitraria – riducendolo a una stringa di lunghezza fissa. Tale stringa, chiamata valore di *hash* e anche detta *checksum* crittografico o *message digest*, costituisce l'impronta digitale univoca che caratterizza il documento sottoposto al processo di *hashing*.

La creazione di tale stringa – che più semplicemente è costituita da una serie prefissata di bit frutto della traduzione mediante calcolo di *hash* del testo originale – permette di verificare che non vi siano state modifiche, anche accidentali, sul dato digitale che si analizza. Per la verifica è sufficiente paragonare la stringa che si sta esaminando con quella del documento dalla quale è stata estratta copia: se le due stringhe risultano identiche significa che vi è altresì identicità del contenuto digitale sul quale sono state apposte, con conseguente certezza riguardo all'integrità.

Inoltre, la funzione di *hash* si rivela uno strumento efficace anche in chiave di semplificazione e riduzione temporale. Se infatti è possibile estrarre più copie forensi del dispositivo sorgente mediante *bit stream image*, è altrettanto vero che la lentezza di questo metodo comporta tempi non indifferent e non previene il rischio cui la memoria da acquisire resta soggetta, consistente nella possibilità che possa subire alterazioni non volute, così portando alla creazione di copie forensi divergenti tra loro.

La funzione di *hash* in parte ovvia a queste problematiche, poiché, una volta calcolatone il valore sulla copia, sarà possibile procedere direttamente alla duplicazione della copia medesima, estraendo in buona sostanza ulteriori copie dalla copia. Per verificare la correttezza della copia, infatti, sarà sufficiente leggere in comparazione il valore di *hash*.

La disciplina nazionale alla luce della L.n. 48 del 2008: best practices e standard internazionali

Già a partire dagli ultimi decenni del secolo scorso, il legislatore ha iniziato ad attenzionare le dinamiche giuridiche connesse al mondo dell'informatica, anche nell'ambito penalistico giungendo, su impulso della Raccomandazione n. 9 del 1989 del Consiglio d'Europa[34], alla promulgazione della legge n. 547 del 1993, rubricata *"Modificazioni ed integrazioni alle norme del Codice penale e del Codice di procedura penale in tema di criminalità informatica"*. Ma l'attuazione di previsioni normative specifiche concernenti la materia della *digital forensics* si è avuta solamente più avanti nel tempo: è solo con la legge n. 48 del 2008, di ratifica ed esecuzione della "Convenzione di Budapest" del Consiglio di Europa sulla criminalità informatica (firmata nella capitale ungherese in data 23 novembre 2001[35]), che è stata inserita nell'ordinamento nazionale una disciplina focalizzata, oltreché sulla previsione del crimine informatico in sé, anche sul procedimento di

[34] M. LIMONE, *"Cloud computing – aspetti contrattuali, risvolti normativi e tutela della privacy"*, Tricase (LE), 2018, p. 10, come citato in R. MURENEC, op. cit., p. 25, dove si precisa che detta raccomandazione, successiva a quella del 30 aprile 1980 del medesimo organo denominata *"informatica e diritto"*, già a partire dal 1989 invitava i paesi UE ad integrare le proprie singole legislazioni con normative *ad hoc* in contrasto a fenomeni criminosi come l'accesso abusivo a sistemi informatici e frodi informatiche

[35] La Convenzione di Budapest rappresenta la prima normativa proveniente da un organo dell'Unione Europea volta a disciplinare il settore giuridico del *cybercrime* e delle investigazioni digitali col chiaro obiettivo di uniformare le legislazioni dei paesi europei in merito al contrasto del fenomeno della criminalità informatica, avente per sua natura uno spiccato connotato di transnazionalità. Ad oggi la Convenzione è stata firmata dalla quasi totalità dei paesi europei. In Italia l'iter di ratifica è iniziato l'11 maggio 2017 e si è concluso con la promulgazione della legge n. 48 del 2008 e con la sua entrata in vigore il 5 aprile del medesimo anno, sebbene con qualche iniziale incertezza relativamente alla data di entrata in vigore fugata dal chiarimento della Suprema Corte Sent. Cass., II Sez., n. 11135 del 13 marzo 2009, pronunciatasi in conferma del giorno del 5 aprile. Per un resoconto più dettagliato, sul punto si veda S. ATERNO, op. cit., pp. 784-785.

acquisizione delle evidenze digitali rinvenute all'interno di sistemi informatici e sulla loro successiva conservazione.

Per quel che riguarda tali materie, la legge di ratifica della Convenzione ha avuto l'onere di dover apportare concetti innovativi in un quadro codicistico, quale quello del codice di procedura penale attualmente vigente e risalente al 1988, inserendovi una tematica, per l'appunto la ricerca della prova informatica, difficilmente imprevedibile al momento della sua entrata in vigore. Nel fare ciò, la l. 48 del 2008 ha operato una serie di modifiche al Titolo III del Libro III e al Titolo IV del V del codice di rito introducendo nuove disposizioni in tema di ispezione, perquisizione e sequestro di supporti informatici nonché di acquisizione e conservazione delle evidenze digitali in essi rinvenute.

In particolare, per quanto riguarda il Titolo III del Libro III c.p.p. in tema di mezzi di ricerca della prova, le modifiche hanno interessato gli artt. 244, 247 (al quale è stato aggiunto il comma 1 bis), 248, 254 (a seguito del quale è stato inoltre inserito l'art. 254 bis), 256, 259-260 e, per quanto riguarda il Titolo IV del Libro III in tema di attività a iniziativa della polizia giudiziaria, gli artt. 352, 353 e 354.

Per ciò che concerne strettamente la materia della *digital forensics*, nell'introdurre le novità normative, la strategia del legislatore non è stata inserire tra le norme codicistiche disposizioni volte a indicare nel dettaglio le modalità per effettuare ispezioni o perquisizioni su supporti informatici, ovvero per eseguirne il sequestro. Infatti, né all'interno del codice né di altre fonti legislative sono state inserite specifiche procedure obbligatorie che le persone deputate alle operazioni, si tratti dellla polizia giudiziaria o di un consulente tecnico, debba seguire e rispettare, a pena di nullità, per visionare, acquisire, analizzare e conservare le evidenze informatiche.

Si è invece optato per una soluzione maggiormente flessibile, che di fatto lascia all'operatore un'ampia libertà di scelta in merito alla migliore modalità da adottare in relazione al caso concreto che gli si propone di volta in volta.

Nello specifico, la l. 48 ha stabilito – mediante apposite interpolazioni all'interno degli artt. 244 sull'ispezione informatica, 247 co. 1 bis sulla perquisizione informatica, 254 bis e 260 sul sequestro di supporti informatici e apposizione dei sigilli, nonché 352 e 354

sulla perquisizione e sequestro urgenti dei medesimi – che nel condurre tali attività, in caso di ispezioni e perquisizioni, occorre procedere *«adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»* (art. 244 co. 2, 247 co. 1 bis e 352 co. 1 bis c.p.p.) e che, per eseguire il sequestro di dati digitali, è necessario che *«la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità»* (artt. 254 bis, 260 e 354 c.p.p.).

Quindi, nell'ottica della legge in questione, ciò che occorre fare non è attenersi a percorsi prestabiliti: è semplicemente agire adottando tecniche volte a non alterare il dato, al fine di conservarne l'autenticità e l'attendibilità. In pratica la legge n. 48 del 2008, senza imbrigliare l'operatore in modalità precise, si è limitata ad inserire nel codice esclusivamente l'obbligo di seguire delle linee guida generali, aperte all'innovazione (si tenga presente che le linee guida possono cambiare, oltre che in relazione alla situazione, anche con il progresso tecnologico), finalizzate a garantire la salvaguardia dell'integrità del dato digitale e la sua successiva verificabilità, a pena di inutilizzabilità processuale dello stesso[36].

Difatti, mediante la normativa in questione, è stato introdotto nel nostro ordinamento l'obbligo per le autorità inquirenti di fare ricorso, in caso di ispezioni, perquisizioni o sequestri di supporti e dati informatici, alle c.d. *best practices*, intese come *«quel comportamento, non necessariamente codificato o contenuto in manuali, che è ritenuto dalla comunità scientifica e dagli operatori tecnici come la modalità corretta per effettuare determinate operazioni informatiche su specifici dispositivi o supporti»*[37].

Più specificamente, le *best practices* vanno considerate veri e propri principi guida[38] cui conformarsi al fine di dare credibilità alle operazioni svolte sui dati informatici. Principi che lasciano tuttavia un certo grado di manovra al soggetto che materialmente conduce

[36] F. GIUNCHEDI, "Le malpractices nella digital forensics Quali conseguenze sull'inutilizzabilità del dato informatico?", in Archivio Penale, settembre–dicembre 2013, fasc. 3, anno LXV, p. 825.

[37] A. COLAIOCCO, *"La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria"*, in Archivio Penale – Cultura penale e spirito europeo, n. 1 del 2019, p. 2.

[38] *Ibidem*

l'acquisizione della *digital evidence*, il quale avrà dunque un margine di apprezzamento circa le modalità da adottare; anche se, in ogni caso, dovrà attuare quelle ritenute migliori in relazione al caso concreto, sempre nell'ottica di garantire l'integrità del dato e la genuinità del risultato finale, *«adottando le misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»* (art. 244 co. 2, 247 co. 1 bis e 352 co. 1 bis c.p.p.) e facendo ricorso a *«…una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità»* (artt. 254 bis, 260 e 354 c.p.p.).

In dottrina, i principi cardine delle *best practices* sono stati riassunti come segue: *«adottare estrema cautela nel sequestrare computer o servizi informatici che muovono servizi di telecomunicazione critici, e prediligere, se possibile, la continuità aziendale effettuando copie su supporti adeguati e non interrompendo, così, l'azione delle macchine e dei servizi; prestare attenzione a non alterare i dati durante le operazioni di ricerca delle fonti di prova; quando si effettua una duplicazione, assicurarsi che siano garantite la conformità della copia all'originale e la sua immodificabilità»*. In termini più diretti, quindi, *«corrette modalità di conservazione, procedure di duplicazione efficaci, garanzie di non alterabilità ed extrema ratio del sequestro di servizi sono, in conclusione, i quattro principi della forensics introdotti nel nostro ordinamento»*[39].

Se da un lato la scelta di non disciplinare procedure di *digital forensics* dettagliate risulta corretta, poiché situazioni differenti potrebbero necessitare di approcci differenti (nonché in ragione della moltitudine di scenari che occorrerebbe prevedere a livello normativo), da altro lato va sottolineato come venga lasciato ampio spazio interpretativo all'autorità procedente.

Proprio in ragione di ciò, a livello internazionale è stata avvertita l'esigenza di creare degli standard, c.d. S.O.P. (*Standard Operating Procedure*)[40], capaci di indicare delle linee guida

[39] G. ZICCARDI, *"L'ingresso della computer forensics nel sistema processuale italiano"*, in *"Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008, n. 48)"* a cura di L. LUPARIA, Milano, 2009, p. 170, come citato in A. COLAIOCCO, op. cit., pp. 2 e 3.

[40] Le *S.O.P.* son definibili come dei documenti che forniscono appositi standard operativi indicando i passaggi chiave di determinate procedure e le regole per eseguirli correttamente.

generali fruibili da chiunque e di individuare i passaggi chiave rispetto ai quali una buona indagine che applichi strumenti di *digital forensics* non può prescindere per garantire un risultato certo in termini di integrità della *digital evidence* e conoscibilità delle varie fasi operative per una loro verifica *ex post*.

Premesso che a livello nazionale non esiste uno standard universalmente seguito da tutte le autorità inquirenti[41], le quali applicano modalità operative differenti nell'espletamento delle rispettive funzioni, gli standard maggiormente utilizzati e dai quali maggiormente viene preso spunto sono gli standard ISO/IEC[42]:

- Standard ISO/IEC 27037:2012 (Information security management systems);
- Standard ISO/IEC 27000:2013 (Guidelines for identification, collection, aquisition and preservation of digital evidence);
- Standard ISO/IEC 27041:2015 (Guidances on assuring suitability and adequacy of incident investigative method);
- Standard ISO/IEC 27042:2015 (Guidelines for the analysis and interpretation of digital evidence);
- Standard ISO/IEC 27043:2015 (Incident investigation principles and processes);
- Standard ISO/IEC 27050:2019, diviso in quattro parti e concernente l'electronic discovery.

Esistono anche altri standard elaborati da enti diversi, aventi in ogni caso tuttI il medesimo obiettivo: garantire l'attendibilità, sotto i differenti aspetti, delle attività di *digital forensics* e dunque delle risultanti *digital evidence*.

Elemento comune tra gli standard internazionali è l'indicazione, all'interno delle loro linee

[41] F. Per un esempio di modalità operative di *digital forensics* di una forza di polizia del nostro Ordinamento si veda G. COSTABILE, op. cit., pp. 20 e ss., dove viene riportato l'esempio delle procedure tecniche delle quali si serve la Guardia di Finanza, basate sulla Circolare GdF 1/2018 denominata *"Manuale operativo in materia di contrasto all'evasione e alle frodi fiscali"*.

[42] *Cfr.* Ivi, pp. 8 e ss. dove vengono elencati e analizzati i principali standard ISO/IEC, con particolare riferimento allo standard ISO/IEC 27037:2012.

guida, di alcuni soggetti specifici chiamati a intervenire: il *Digital Evidence First Responder* (DEFR), ovvero chi per primo fornisce il proprio intervento sulla scena del crimine ed eventualmente, se non vi è possibilità di dilazionare le operazioni, procede all'acquisizione del materiale digitale rinvenuto, e il *Digital Evidence Specialist* (DES), il soggetto dotato delle competenze tecniche di settore e chiamato ad attuare le procedure della *digital forensics* (che può coincidere con la figura del DEFR[43]).

L'attenzione delle S.O.P. richiamate, in particolare dello standard ISO/IEC 27037:2012[44], si è concentrata anche nell'indicazione metodica e cronologica delle fasi del processo di *digital forensics*, con l'individuazione di un modello procedurale dettagliatamente definito. Nello specifico l'intero procedimento viene sistematicamente suddiviso in passaggi ben distinti gli uni dagli altri, sebbene concatenati tra loro secondo un ordine logico-temporale.

Tali fasi si articolano come segue:

- identificazione della *digital evidence* nel contesto della presunta *scena criminis*;
- raccolta, acquisizione e analisi del materiale informatico raccolto;
- valutazione del medesimo in base alle esigenze d'indagine.

Tutti i passaggi vanno attuati tenendo a mente i principi cardine della catena di custodia, volti a conseguire una corretta gestione dei dati – e dei supporti dai quali sono estratti – durante la loro manipolazione, al fine di tutelarne l'integrità durante ciascuna fase e nei momenti di passaggio dall'una all'altra.

[43] S. ATERNO, op. cit., p. 783, dove si specifica che in Italia non è consentita la coincidenza tra i due soggetti e pertanto la figura del *first responder* nel nostro Ordinamento è da rinvenirsi in quella del primo investigatore interveniente sulla scena, mentre quella del *Digital Evidence Specialist* è invece assimilabile al consulente specialista. Si veda anche R. MURENEC, op. cit., p. 217, dove tale ultima figura viene denominata *Digital Forensics Expert* e qualificata come *"la figura professionale esperta di crimini informatici che si occupa di identificare, preservare e analizzare le informazioni contenute all'interno di dispositivi digitali [… al fine di] raccogliere elementi probatori…"*. Come da quest'ultimo autore citato si veda altresì A. CONTALDO e F. PELUSO, *"E-detective: l'informatica giuridica e le applicazioni della Digital Forensics"*, PM Edizioni, Verazze (SV), 2018, p. 201 e ss., dove vengono evidenziati ulteriori approfondimenti su tale figura.

[44] Si segnala che lo standard ISO/IEC 27037 negli anni ha subito degli aggiornamenti. Attualmente l'ultima versione è quella del 2017, la quale a sua volta ha recepito la versione del 2016.

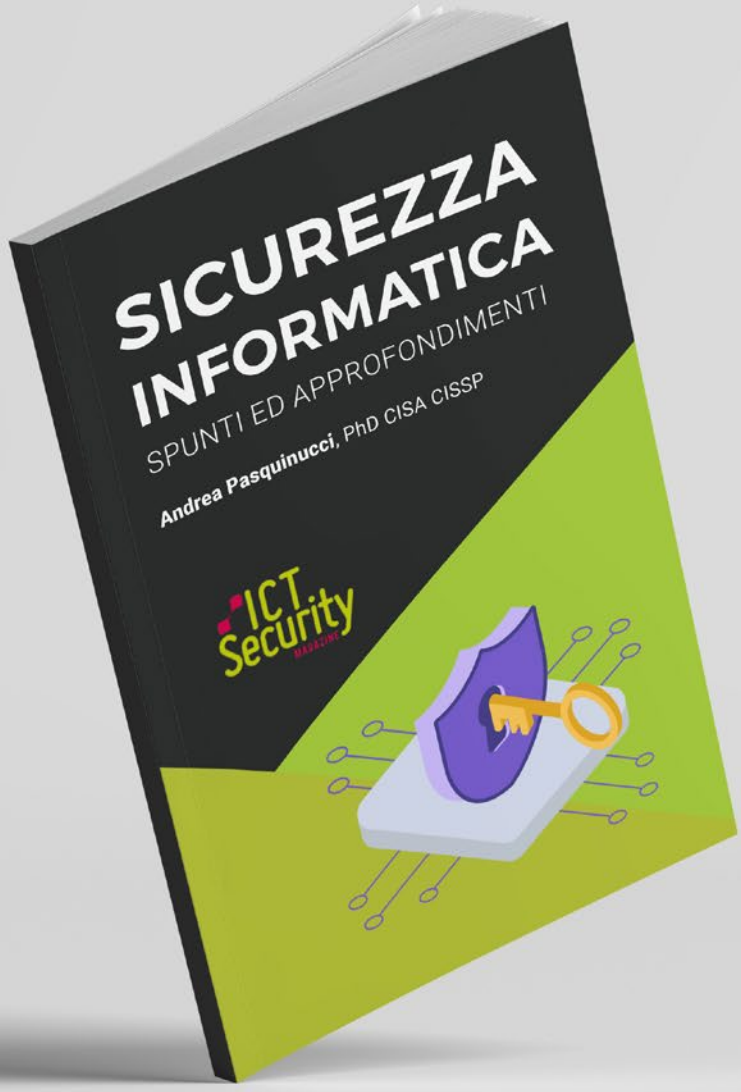
Parte della dottrina[45] ha ravvisato l'esigenza di aggiungere un ulteriore step a conclusione dell'intero processo, consistente nella presentazione all'autorità inquirente/giudiziaria, o anche al difensore della persona indagata, del risultato ottenuto dal reperto informatico dopo averlo analizzato e valutato. Infatti occorre sottolineare che il processo di *digital forensics* e la lettura delle determinazioni ricavate dalle *digital evidence* che vi si estrapolano sono dotati di un alto grado di tecnicità, tale da risultare di difficile comprensione per l'"utente finale". Soggetto, quest'ultimo, molto spesso esterno al settore e al quale i risultati investigativi andranno esposti con un linguaggio accessibile, ai fini del loro corretto utilizzo in sede processuale.

[45] In tal senso si vedano G. COSTABILE, op. cit., p. 9 e S. ATERNO, op. cit., p. 781.

Libro in versione **cartacea** ed **eBook**

SICUREZZA INFORMATICA

SPUNTI ED APPROFONDIMENTI



Il libro è distribuito gratuitamente a tutti gli iscritti alla newsletter di ICT Security Magazine

Conseguenze in caso di violazione delle *best practices*: la sentenza Vierika

Oltre a non aver disciplinato in dettaglio il processo di digital forensics ma avendo scelto, come visto, di lasciare libero ingresso nell'ordinamento alle c.d. *best practices*, il legislatore non si è nemmeno preoccupato di fare riferimento a conseguenze specifiche in caso di violazione delle medesime durante il trattamento del reperto informatico.

Infatti mancano, tra le novità apportate dalla legge del 2008, delle previsioni specifiche concernenti le conseguenze in caso di violazione delle misure tecniche cui il codice fa riferimento al fine di garantire la protezione e l'integrità delle *digital evidence*. Norme peraltro non rinvenibili nemmeno all'interno di interventi legislativi successivi.

Di conseguenza la dottrina, sin dal primo momento, si è posta il problema della validità processuale delle evidenze digitali trattate in violazione delle *best practices* comunemente accettate dalla comunità di settore. Nello specifico ci si è domandati quale potesse essere la sanzione da applicare nei confronti di elementi probatori ottenuti mediante "*malpractices*".

Un primo filone di pensiero ipotizza, al riguardo, la sanzione giuridica della nullità a norma dell'art. 178, lett. c) c.p.p.[46] in quanto l'impiego di evidenze estratte o conservate in difformità rispetto ai canoni standardizzati dalle "migliori procedure" arrecherebbe un grave pregiudizio alle garanzie difensive del soggetto sottoposto a processo.

[46] A. VITALE, *"La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico"*, in Dir. Internet, 2008, p. 509, come citato in F. CAJANI, *"Il vaglio dibattimentale della digital evidence"*, in Archivio Penale, settembre-dicembre 2013, fasc. 3, anno LXV, pp. 838 e 839, dove l'autore osserva che la sanzione della nullità in una simile situazione sarebbe stata già propugnata prima dell'entrata in vigore della legge n. 48 del 2008 dal Tribunale di Vigevano in merito al caso Garlasco.

Secondo una visione più "morbida", in questi casi non andrebbero automaticamente applicate delle sanzioni processuali ma il giudizio sulla validità della prova informatica andrebbe lasciato all'apprezzamento dell'organo giudicante, in sede di valutazione della prova ex art. 192 c.p.p.[47] Posizione nei confronti della quale è stata mossa la netta opposizione per cui, in caso di malpractices, il libero convincimento del giudice verrebbe influenzato da una raccolta probatoria eseguita non correttamente e che, dunque, sottoporrebbe al suo vaglio decisionale degli elementi probatori erronei[48].

Un'ultima prospettiva dottrinale ha ravvisato nell'inutilizzabilità processuale ex art. 191 c.p.p. la sanzione maggiormente adeguata, giacché le modifiche apportate con l. 48/2008 non andrebbero considerate *«mere indicazioni operative prive di alcuna sanzione, ma veri e propri divieti impliciti presidiati dalla sanzione dell'inutilizzabilità»*[49].

Di tutt'altro avviso la giurisprudenza, dove si è registrata una tendenza favorevole al riconoscimento della piena validità e utilizzabilità, "fino a prova contraria", del dato informatico seppure ricavato con procedure che non collimano con quelle enunciate dagli standard internazionali.

Per chiarire meglio, secondo la giurisprudenza prevalente i dati acquisiti e conservati con l'utilizzo di metodologie non indicate in protocolli riconosciuti possono comunque avere una piena validità processuale, fintanto che non siano portati all'attenzione del giudice elementi idonei a dimostrare come dette procedure abbiano compromesso in qualche modo l'integrità della prova informatica. In buona sostanza, l'unico modo per inficiare il valore probatorio delle evidenze digitali sarebbe provare che le attività degli inquirenti, per come svoltesi, abbiano concretamente potuto alterare la genuinità del reperto digitale. Ovviamente, in questa visione prospettica, il compito di scovare eventuali falle nell'operato degli inquirenti spetterebbe alla difesa, la quale fisiologicamente interviene (quasi

[47] Si vedano M. DANIELE, op. cit., pp. 288 nonché ss., F. CAJANI, op. cit. e G. BRAGHÒ, "L'ispezione e la perquisizione di dati, informazioni e programmi informatici", in L. LUPARIA, op. cit., p. 190, come citati in A. COLAIOCCO, op. cit., p. 3.

[48] Si vedano L. MARAFIOTI, op. cit., p. 4517 nonché E. LORENZETTO, "Le attività urgenti di investigazione informatica e telematica", in L. LUPARIA, op. cit., p. 162, come citati in A. COLAIOCCO, op. cit., p. 3.

[49] M. PITTIRUTI, op. cit., p. 159 come citato in A. COLAIOCCO, op. cit., p. 4.

sempre) a operazioni già concluse.

Per la giurisprudenza, dunque, almeno in linea teorica, non sono gli organi inquirenti a dover dimostrare di aver agito correttamente seppure senza aver seguito le prassi indicate dalle *best practices*, bensì, mediante una sorta di inversione dell'onere della prova, spetta all'imputato, *ex post,* il compito di far emergere eventuali errori nell'operato dell'accusa, oppure direttamente al giudice medesimo in fase di valutazione della prova. Tali errori, peraltro, devono "concretamente" aver inciso negativamente sull'evidenza informatica, dovendosi palesare il rischio di una sua avvenuta adulterazione.

In tal senso appaiono emblematiche le pronunce relative alla vicenda processuale del noto caso Vierika, con riguardo sia al primo grado[50] che al relativo appello[51]: entrambe antecedenti (anche se di soli pochi giorni per la sentenza di appello) all'effettiva entrata in vigore della legge n. 48/2008 ma contenenti soluzioni giuridiche che hanno segnato un punto di riferimento per la giurisprudenza successiva.

Il caso in esame verteva sulle modalità con cui era stata condotta l'estrazione di dati informatici dai supporti interessati dall'indagine, in un procedimento penale concernente un'ipotesi di accesso abusivo a sistema informatico o telematico *ex* art. 615 ter c.p. e per danneggiamento di sistema informatico o telematico *ex* art. 615 quinquies c.p., mediante l'utilizzo di un virus informatico che sarebbe stato creato dall'imputato e denominato per l'appunto "Vierika".

L'acquisizione dei dati era stata effettuata mediante estrazione di copia degli stessi, direttamente sul luogo ove i supporti erano ubicati, ad opera del soggetto indagato, sotto la sorveglianza degli operanti di polizia giudiziaria che avevano accordato tale modalità assecondando la richiesta dell'indagato.

È proprio sulla peculiarità di tale modalità procedurale che si fondavano le tesi difensive. Per la difesa, infatti, questa modalità non sarebbe stata tale da garantire la genuinità delle informazioni copiate e portate in dibattimento per sostenere gli assunti dell'ac-

[50] Tribunale di Bologna, Sent. n. 1823 del 22 dicembre 2005.

[51] Corte di Appello di Bologna, Sent. n. 369 del 27 marzo 2008.

cusa, trattandosi di una procedura connotata da spiccata singolarità, tale da lasciare dubbi sull'integrità dei dati acquisiti e svolta in assenza di un reale contraddittorio con gli esponenti della difesa. Veniva pertanto richiesto l'espletamento di ulteriori accertamenti peritali; richiesta disattesa dal giudice, che valutava il materiale probatorio così reperito come attendibile e pienamente utilizzabile.

In particolare, usando le parole della sentenza *«non è compito di questo Tribunale determinare un protocollo relativo alle procedure informatiche forensi, ma semmai verificare se il metodo utilizzato dalla p.g. nel caso in esame abbia concretamente alterato alcuni dei dati ricercati»*.

Altrettanto significativo il passaggio in cui il magistrato, riferendosi alle affermazioni della difesa circa l'esistenza di procedure migliori rispetto a quelle adottate, chiariva che *«non è permesso al Tribunale escludere a priori i risultati di una tecnica informatica utilizzata a fini forensi solo perché alcune fonti ritengono ve ne siano di più scientificamente corrette, in assenza della allegazione di fatti che suggeriscano che si possa essere astrattamente verificata nel caso concreto una qualsiasi forma di alterazione dei dati e senza che venga indicata la fase delle procedure durante la quale si ritiene essere avvenuta la possibile alterazione»*.

In estrema sintesi, stando alla pronuncia, in assenza della prova che i dati repertati abbiano subito effettivamente delle alterazioni i medesimi sono pienamente utilizzabili e devono essere lasciati alla valutazione del giudice, anche qualora il metodo di acquisizione adottato non sia stato tra i migliori.

In termini più generali, quindi, il materiale probatorio raccolto dagli inquirenti è da considerarsi valido anche in caso di discostamento dalle *best practices*, a meno che, in qualche modo, non si riesca a dimostrarne l'adulterazione. Ciò poiché il giudice è esclusivamente tenuto a verificare che durante l'acquisizione non si siano prodotte alterazioni, non dovendo invece sindacare sulla procedura materialmente adottata. Ragionamento che, per estensione, potrebbe essere applicato a tutte le fasi del processo di *digital forensics*.

La tesi accolta nel primo grado di giudizio veniva sostanzialmente accolta anche nel relativo appello, attivato su ricorso presentato dalla difesa, ove il collegio, oltre a rigettare

la richiesta di nuova perizia e a pronunciarsi in senso favorevole alla corretta formazione del contraddittorio giacché *«con l'accordo delle parti, sono state acquisite ex art. 493, c.3, c.p.p., e dichiarate utilizzabili per la decisione le annotazioni di polizia giudiziaria»*, ribadiva che «non è compito del giudicante determinare una sorta di protocollo delle procedure informatiche forensi, ma solo verificare se nella fattispecie l'acquisizione probatoria sia fidefaciente, o se abbia subito alterazioni».

Come anticipato, l'interpretazione fornita dalle pronunce relative al caso Vierika ha rappresentato un punto di riferimento anche per la giurisprudenza successiva.

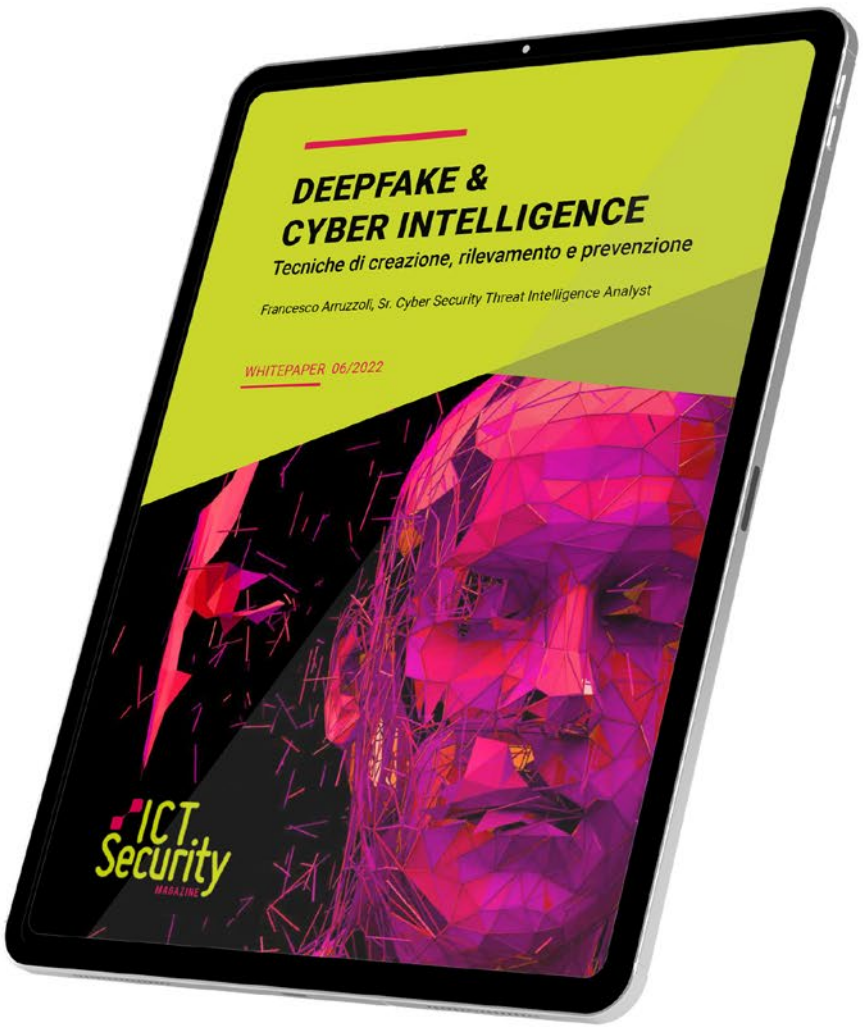
Vista con sguardo critico tale posizione lascerebbe trasparire la non necessità, nello svolgimento delle varie fasi della *digital forensics*, di attenersi forzatamente alle pratiche migliori tracciate dagli standard internazionalmente riconosciuti, così riducendo la rilevanza delle *best practices* all'interno dell'ordinamento nazionale. Per altri versi, invece (come già paventato da parte della dottrina[52]), si rischierebbe di far penetrare all'interno del giudizio degli elementi di prova che potrebbero essere frutto di una raccolta erronea, difficilmente verificabile e di conseguenza tale da poter influenzare il convincimento del giudice, anche in considerazione delle conoscenze tecniche, spesso aliene alle competenze di figure esterne al settore digitale, che servono per poter valutare il corretto svolgimento di procedure informatiche.

[52] Si vedano L. MARAFIOTI, op. cit., p. 4517 e E. LORENZETTO, op. cit., p. 162, come citati in A. COLAIOCCO, op. cit., p. 3.

White Paper

DEEPFAKE & CYBER INTELLIGENCE

Download gratuito su www.ictsecuritymagazine.com



Atti ripetibili e irripetibili nella *digital forensics*

Il problema della fragilità del reperto informatico, data l'estrema capacità di modificazione che lo connota, ha interessato i giuristi anche con riguardo al tema della ripetibilità o irripetibilità delle relative operazioni.

In particolare, ci si è chiesti se tali fasi siano assistite dalle tutele previste dall'art. 360 c.p.p. e debbano dunque essere considerate accertamenti irripetibili[53], con la necessità di ricorrere alle conseguenti garanzie procedurali, oppure se siano riconducibili all'art. 359 c.p.p. e quindi da considerarsi accertamenti ripetibili[54]. Ci si è domandati, insomma, se e quali attività debbano essere assistite dalle garanzie proprie degli atti irripetibili (e quali invece no).

Premesso che in determinate situazioni la scelta della modalità attuativa potrebbe essere influenzata dalla tipologia di supporto informatico attenzionato e in altre imposta da un'urgenza improrogabile, che non consentirebbe l'instaurazione del contraddittorio *ex* art 360 c.p.p., occorre evidenziare una prima distinzione che potrebbe delinearsi tra momento dell'estrazione in copia forense dal supporto originale (fase di acquisizione *tout court*) – dove la linea di demarcazione tra accertamento ripetibile e irripetibile è meno nitida – e

[53] Per accertamenti irripetibili si fa riferimento a quel tipo di accertamento da eseguire su «persone, cose o luoghi il cui stato è soggetto a modificazioni» (art. 360, co. 1, c.p.p.). Si tratta pertanto di quegli accertamenti che, sussistente un rischio concreto di modificazione, non consentono di essere rinviati ad altro momento, o che possono essere eseguiti una volta sola e che per poter essere espletati necessitano della messa in essere di dettagliate procedure poste a garanzia della difesa, prima fra tutte l'instaurazione del contraddittorio.

[54] Per accertamenti ripetibili ci si riferisce a quelle attività consistenti in «accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze tecniche...» (art. 359 c.p.p.) che possono essere ripetuti più volte e che pertanto non necessitano della formazione del contraddittorio per essere espletati.

momenti successivi all'estrazione della copia forense, con riguardo agli atti compiuti sulle copie stesse.

Per quanto riguarda questo secondo caso, non sembra esserci dubbio in merito alla ripetibilità delle operazioni: una volta cristallizzate le *digital evidence* è possibile creare molteplici "cloni da lavoro" direttamente dalla beat stream image stessa, dalla quale si potrà quindi partire per svolgere (e ripetere) tutti gli accertamenti successivi necessari al completamento delle investigazioni, così salvaguardando il supporto originale che potrà essere impiegato per attuare verifiche sulla sua integrità.

La questione diventa più intricata nel momento dell'estrazione della prima copia, che avviene – per l'appunto – direttamente dal supporto originale; momento in cui qualunque errore, anche involontario, potrebbe irrimediabilmente compromettere il contenuto digitale del sistema da acquisire, così falsando inevitabilmente l'acquisizione. Un momento, dunque, dove l'instaurazione del contraddittorio propria degli accertamenti tecnici irripetibili consentirebbe alla difesa di partecipare a tutela dell'indagato.

Esclusi dunque quei casi di assoluta urgenza, nei quali l'esigenza di procedere si paleserebbe improrogabile a causa di situazioni di rischio che non consentirebbero di dilazionare le operazioni in attesa della difesa, occorre capire se le forme contemplate dall'art. 359 c.p.p. siano idonee a salvaguardare la posizione della persona sottoposta alle indagini e, più in generale, il corretto andamento del processo.

Sul piano giuridico, si tratta di capire se l'acquisizione delle *digital evidence* rientri nella categoria degli "accertamenti tecnici", cioè quelle operazioni che comportano un'opera di studio critico, valutazione o giudizio dei reperti; oppure se si tratti piuttosto di un'attività di mero "rilievo tecnico", attinente la semplice individuazione, raccolta e acquisizione del materiale[55].

[55] Una simile distinzione tra il concetto di accertamenti tecnici e rilievi tecnici è stata formulata dalla Suprema Corte già a partire dai primi periodi di vita dell'attuale codice di procedura penale, con un orientamento pressoché costante, anche con riferimento alla prova scientifica. Per una delle prime pronunce si veda Cass. Pen., Sez. I, n. 301 del 14 marzo 1990. Tra le altre, anche Cass. Pen., Sez. I, n. 239101 del 16 gennaio 2008 e Cass. Pen., Sez. IV, n. 637 del 14 aprile 2004.

In proposito parte della dottrina, in ottica garantista e sul presupposto dell'inesistenza di una previsione che comporti l'inutilizzabilità del dato digitale ottenuto in violazione delle *best practices*, ha prospettato come soluzione migliore quella del ricorso alle procedure imposte dall'art. 360 c.p.p., annoverando l'acquisizione nella categoria degli accertamenti tecnici irripetibili[56].

Effettivamente, in tal maniera alla difesa sarebbe consentito di assistere alle procedure di estrazione: così, da un lato, si tutelerebbero quanto più possibile i diritti difensivi e, dall'altro, si imprimerebbe ai dati informatici acquisiti una certa attendibilità, conferita proprio dal contraddittorio instaurato tra le parti, eventualmente alla presenza di un consulente tecnico nominato dalla difesa[57].

Di impostazione diametralmente opposta, tuttavia, la giurisprudenza maggioritaria.

Per orientamento consolidato della Suprema Corte di Cassazione, infatti, la formazione del contraddittorio nel momento dell'estrazione della copia forense non è condizione essenziale per l'espletazione delle operazioni di *digital forensics*, giacché la creazione della *bit stream image*, qualora venisse fatto ricorso a metodi atti ad impedire alterazioni e danneggiamenti dei dati, deve essere ricompresa nella categoria dei semplici "rilievi". Ciò poiché l'estrazione di dati digitali non presupporrebbe attività valutative o di giudizio critico, non ponendosi quindi problemi in relazione alla ripetibilità ex art. 359 c.p.p.[58].

[56] Tra le altre voci in tal senso si veda F. GIUNCHEDI, op. cit., pp. 828 e 829, dove il ricorso alla procedura dell'accertamento tecnico non ripetibile viene descritta come una via «*precauzionale*».

[57] *Ibidem*, dove ci si sofferma sul verbo "assistere" utilizzato dall'art. 360 c.p.p. e al significato da attribuirvi in sede di acquisizione. Per l'autore, in particolare, quando si procede ad acquisizione di dati digitali *«Il punto è chiarire il significato da attribuire al verbo «assistere» ed in particolare se poterlo ritenere quale prologo al successivo diritto di formulare osservazioni e riserve. Se, infatti, lo si intende come attività di osservazione passiva, volta sul piano processuale a verificare la regolarità del compimento degli atti, è ovvio che il diritto di difesa risulta seriamente compromesso; diverso è il caso in cui l'accertamento tecnico ex art. 360 c.p.p. sia da assimilarsi per analogia alla perizia; qui il termine assistenza va letto in termini più ampi – di contraddittorio – e in correlazione logica con i diritti successivamente assicurati (partecipazione agli accertamenti, formulazione di osservazioni e riserve). L'art. 226, co. 2 c.p.p. prevede, infatti, un contraddittorio nella formulazione dei quesiti («Il giudice formula quindi i quesiti, sentiti il perito, i consulenti tecnici, il pubblico ministero e i difensori presenti»)».*

In buona sostanza, *«ciò che sposta il confine tra atto ripetibile e atto irripetibile è l'attenta acquisizione dei dati dal supporto originale e la possibilità di provare successivamente a livello scientifico che i dati della copia effettuata siano identici (in senso informatico) a quelli originali e che il supporto originale nel frattempo o durante le operazioni non sia stato modificato o alterato»*[59].

Il quadro descritto, tuttavia, potrebbe assumere tratti di incertezza allorché da una parte la giurisprudenza ammette la ripetibilità dell'acquisizione della copia forense – a patto che sia stata ottenuta con procedure che tutelino l'integrità dei dati – mentre dall'altra parte, come visto con il caso Vierika, accetta di far pervenire all'attenzione del giudice elementi ottenuti in omissione del rispetto delle *best practices* internazionali richiamate dalla legge n. 48/2008. Nuovamente, quindi, si correrebbe il rischio di lasciare al giudice il compito di valutare un materiale probatorio che potrebbe essere frutto di una raccolta erronea, lasciando alla difesa l'onere di dover "smontare" un quadro accusatorio costituito da elementi informatici, già per loro natura estremamente fragili, acquisiti senza la sua partecipazione.

[58] Fra le altre pronunce che aderiscono all'orientamento maggioritario si vedano Cass. Pen., Sez. I, n. 14511 del 5 marzo 2009; Cass. Pen., Sez. V, n. 11905 del 16 novembre 2011; Cass. Pen., Sez. I, n. 23035 del 30 aprile 2009. Più recentemente anche Cass. Pen., Sez. V, n. 8736 del 16 gennaio 2018 e Cass. Pen., Sez. VII, n. 11066 del 10 febbraio 2021 dove si legge che *«i dati di carattere informatico contenuti in un computer rientrano tra le prove documentali e per l'estrazione di questi dati non occorre alcuna particolare garanzia; di conseguenza ogni documento acquisito liberamente ha valore di prova, anche se privo di certificazione; sarà poi il giudice a valutarne liberamente l'attendibilità».*

[59] D. CURTOTTI, *"Attività di acquisizione della digital evidence: ispezioni, perquisizioni e accertamenti tecnici"*, in *"Cyber forensics e indagini digitali Manuale tecnico-giuridico e casi pratici"*, cit., p. 445, dove l'autrice, dopo aver analizzato la massima pronunciata da Cass. Pen., Sez. V, n. 11905 del 16 novembre 2011, elabora il passaggio su riportato a sua volta citando S. ATERNO, op. cit., pp. 775 e ss.

Acquisizione della prova informatica all'estero

Il carattere di immaterialità della prova informatica, unito al crescente sviluppo dell'interconnessione digitale, comporta inevitabilmente che l'evidenza digitale da acquisire possa trovarsi all'interno di server ubicati presso paesi differenti da quello ove si svolge l'attività investigativa.

Anche per quanto concerne le indagini portate avanti dall'autorità italiana accade non di rado che, sebbene si proceda per crimini commessi nel nostro territorio, le prove informatiche siano stoccate in sistemi di memorizzazione collocati all'estero[60].

Proprio questo tratto transfrontaliero della *digital evidence*[61] impone un approccio per così dire internazionale, in ottica di cooperazione giudiziaria fra gli Stati. Una corretta comunicazione tra le autorità giudiziarie e le forze dell'ordine dei vari paesi che possono essere coinvolti nelle operazioni di *digital forensics*, infatti, costituisce spesso la chiave di volta per una rapida e buona riuscita dell'indagine, soprattutto per quanto riguarda la fase di acquisizione degli eleemnti di prova.

[60] Sul punto occorre precisare che non sono solo i crimini informatici gli unici idonei a lasciare tracce digitali. Infatti, l'ingerenza che le nuove tecnologie stanno avendo nella quotidianità di chiunque, comporta l'evenienza, cosa che ormai costituisce la normalità, che anche tutti gli altri reati possano avere una loro componente informatica. Basti pensare a reati organizzati su chat online, o a documenti salvati sul dispositivo, etc. Cfr. R. MURENEC, op. cit., p. 115 dove per l'autore *«oggi potrebbe risultare arduo immaginare un crimine che non abbia una dimensione per così dire "digitale"».*

[61] Ivi, p. 116, dove la natura transnazionale della prova digitale viene ricondotta a tre aspetti specifici, ovvero: *«localizzazione e conservazione della prova digitale»* atteso che la prova digitale può essere memorizzata e conservata in qualsiasi parte del mondo; *«sede dell'Internet Service Provider (ISP privato»,* giacché la maggior parte delle prove digitali si trovano nei server di provider privati che spesso possono avere la sede legale presso altri paesi; *«natura transnazionale del presunto crimine»*, poiché può capitare, specie per i crimini informatici, che il reato coinvolga molteplici giurisdizioni con conseguente aggravamento delle attività di raccolta, acquisizione e utilizzo processuale della prova digitale.

Ad ogni modo, allo stato attuale (salvo alcuni tentativi) non vi è ancora stata una reale armonizzazione tra gli ordinamenti giuridici in tema di *digital forensics*, sicché potrebbero verificarsi situazioni di incertezza con riferimento all'attendibilità di evidenze ottenute presso stati esteri ove non vengono rispettati i principi da noi considerati cardine a garanzia della genuinità della prova nonché, più in generale, le regole costituzionali in materia di giusto processo e tutela dei diritti fondamentali della persona.

In assenza di regole condivise lo strumento principale per l'acquisizione all'estero rimane dunque, anche in tema di indagini digitali, la tradizionale rogatoria internazionale, già vigente per l'assunzione degli altri tipi di prova.

Quanto appena detto vale nei rapporti tra Stati non appartenenti alla Comunità Europea. Un'eccezione è infatti rappresentata, per i soli Stati membri, dalla direttiva del Parlamento europeo e del Consiglio n. 41/2014/UE del 2014 – recepita nel nostro ordinamento con decreto legislativo n. 108 del 2017 – che ha istituito la procedura del c.d. ordine europeo di indagine (OEI).

L'OEI, discostandosi dal meccanismo della richiesta proprio della rogatoria internazionale e poggiando le basi sul mutuo riconoscimento delle decisioni e dei provvedimenti delle autorità giudiziarie straniere, segue le logiche dell'ordine ad eseguire[62]. Più propriamente, l'OEI consiste in un provvedimento mediante il quale l'autorità giudiziaria o amministrativa procedente richiede ad altra autorità di un paese membro di svolgere attività di indagine o di assunzione probatoria – che in materia di *digital forensics* può coincidere, appunto con l'acquisizione in copia forense di evidenze digitali – al fine di acquisire informazioni o prove già disponibili presso il paese a cui è rivolto (art. 1, lett. a d.lgs. n. 108 del 2017)[63].

Una volta rivolto allo stato estero, l'OEI viene sottoposto da quest'ultimo a un giudizio di

[62] F. CAJANI, *"La cooperazione internazionale nelle indagini digitali"*, in *"Cyber forensics e indagini digitali Manuale tecnico-giuridico e casi pratici"*, cit., p. 237.

[63] Ivi, p. 238 dove si specifica che l'ambito di applicazione dell'OEI, in ogni caso, si limita esclusivamente agli atti di indagine e agli atti di ricerca della prova espressamente previsti dalla direttiva n. 49/2014/UE.

ammissibilità; in talune circostanze espressamente previste può essere rifiutato[64], mentre in ogni altro caso deve essere eseguito con rapidità.

Per quanto riguarda le regole esecutive dell'OEI la disciplina lascia ampio margine discrezionale allo Stato di emissione, che può prescrivere all'autorità di esecuzione di utilizzare le proprie modalità attuative.

Di conseguenza, parte della dottrina ritiene che le evidenze digitali ottenute senza il rispetto delle prescrizioni indicate dallo Stato di emissione non potrebbero che condurre alla loro inutilizzabilità in sede giudiziale[65]. Secondo tale filone dottrinale, pertanto, anche la violazione delle best practices accolte dal nostro ordinamento con la legge n. 48/2008 comporterebbe un'ipotesi di inutilizzabilità[66], se fossero poste alla base delle modalità di esecuzione.

Infine, non tutte le attività volte all'assunzione della prova digitale all'estero sono sottoposte al regime della rogatoria internazionale o dell'ordine di esecuzione europeo. All'art. 234 bis del c.p.p., infatti è specificato che «*è sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare*».

Il consenso prestato dal titolare del dato informatico, dunque, fa venire meno l'obbligo di adozione delle formalità contemplate dalle procedure sopra analizzate[67]. Sulla base di tale presupposto, l'autorità competente potrà procedere alla raccolta a distanza, senza che si pongano problematiche attinenti all'utilizzabilità, di tutte le evidenze liberamente

[64] Si pensi ad esempio al caso in cui l'OEI avanzi richiesta di svolgimento di attività d'indagine che si pongano in contrasto con i principi e le libertà dei diritti umani sostenute dall'UE, che siano oggettivamente impossibili da portare ad esecuzione, o ancora che si pongano in contrasto con i principi fondamentali dello stato cui si rivolge la richiesta o ne mettano a rischio l'ordine pubblico.

[65] A. COLAIOCCO, op. cit., pp. 8 e ss.

[66] Ibidem, In senso difforme si veda R. MURENEC, op. cit., p. 139 dove, invece, si legge «non determinerebbe nessuna invalidità delle prove raccolte, per converso, la mancata adozione delle Best Practices dell'informatica richieste a livello nazionale, il cui impiego è suscettibile, al più, di riverberarsi sull'affidabilità cognitiva delle prove ottenute».

accessibili al pubblico in rete. Secondo un'interpretazione nemmeno troppo estensiva della norma, la libera accessibilità deve infatti essere letta come un consenso preventivo del titolare del dato all'acquisizione dello stesso.

[67]-Sul punto si veda Cass. Pen., Sez. VI, n. 18907 del 20 aprile 2021, mediante la quale è stata dichiarata la piena validità processuale dell'acquisizione di conversazioni via chat scambiate tra telefoni del tipo blackbarry e protette da sistema pin to pin, decriptate grazie alla collaborazione volontaria del produttore del sistema operativo, avente sede all'estero, senza che siano state attivate le formalità procedurali della rogatoria internazionale

La catena di custodia della *digital evidence*

In linea generale, una volta raccolto il reperto dalla scena del crimine sorge l'esigenza di conservarne l'originale autenticità in tutti i passaggi successivi – anche mediante documentazione dei singoli spostamenti e indicando chi vi entra in contatto – affinché possa giungere inalterato sino al dibattimento e affinché, in tale sede, possa esserne opportunamente verificata l'attendibilità, valutando la corretta applicazione dei principi cardine della c.d. catena di custodia, espressione con cui *«vengono indicati l'insieme di passaggi, formalizzati con un sistema di tracciamento (manuale o elettronico), attraverso i quali il reperto, o meglio i plichi ed i confezionamenti in cui è conservato, transita dalla scena del crimine alla fase del giudizio»*[68].

In altre parole, la catena di custodia è la *«documentazione cronologica che mostra la conservazione dei reperti dal momento della raccolta a quello della produzione in giudizio»*[69] e che permette in sede giudiziale di poter valutare l'attendibilità del reperto sotto i profili della sua integrità e genuinità, o meglio di verificare che durante tutti i passaggi che hanno coinvolto il reperto sia stato salvaguardato l'insieme di informazioni che intrinsecamente possiede[70].

[68] R. GENNARI e L. SARAVO, "*Tecnica, tecnologia e scienza sulle tracce del reato – Le tracce*", in Manuale delle investigazioni sulla scena del crimine, cit., p. 496, dove gli autori specificano che la catena di custodia è meglio nota con il nome inglese *"chain of custody"*. Effettivamente, preme sottolineare come tale fase dell'investigazione forense sia propria degli sviluppi avutisi in tale settore nella prassi dei paesi anglosassoni e in particolare in quella dell'ordinamento nordamericano. Su quest'ultimo aspetto si veda R. MURENEC, op. cit., p. 128, nota (269).

[69] F. COLAIUDA, *"La qualità dell'investigazione sulla scena del crimine – il metodo di lavoro basato sui protocolli operativi e sulle check lists"*, p. 1, consultabile sul sito http://www.associazionelaic.it/wp-content/uploads/2018/07/Colaiuda-3.pdf.

Alla necessità di rispettare i principi della catena di custodia, basilari per la buona riuscita dell'indagine, non fa eccezione nemmeno la prova informatica; caratterizzata, inoltre, da una fragilità che impone un'attenzione ancora maggiore onde impedirne modificazioni involontarie.

Esaurita, dunque, la fase di acquisizione dei dati dal supporto oggetto d'investigazione, le *digital evidence* ottenute devono essere salvaguardate per garantire il loro ingresso all'interno del processo nello stesso stato nel quale sono state rinvenute. A tal fine occorrerà conservare adeguatamente sia la copia forense che tutte le altre copie che potranno essere estratte a partire da quest'ultima.

Allo stesso modo, al fine di assicurare l'integrità dell'intero quadro probatorio, occorre che anche rispetto al supporto originale siano dettagliatamente documentati gli spostamenti e le fasi operative o conservative che lo interessano, dal suo rinvenimento fino al giudizio.

Nonostante la centralità di questa fase, esattamente come avviene per l'acquisizione, non è però rinvenibile una normativa atta a disciplinarne con chiarezza i passaggi.

La sola disposizione cui è possibile fare riferimento, infatti, è contenuta nel comma 2 dell'art. 260 c.p.p., rubricato *"apposizione dei sigilli alle cose sequestrate. Cose deperibili. Distruzione di cose sequestrate"*[71], dove non viene indicata una procedura precisa ma è

[70] R. GENNARI e L. SARAVO, op. cit., p. 497, dove dopo aver individuato quale obiettivo della catena di custodia la salvaguardia delle informazioni contenute dal reperto si precisa che la protezione afferisce a tre aspetti: quello «*Scientifico dovuto alla necessità di preservare le tracce da fenomeni degenerativi e degradativi, nonché da possibili contaminazioni*» (si aggiunge che in ottica di digital forensics potrebbe tradursi come la necessità di evitare alterazioni del dato digitale); quello «Formale» per il quale «*tutte le fasi di custodia, dal repertamento alle analisi di laboratorio, devono essere opportunamente documentate [… al fine di] garantire che non vi sia pericolo di scambio e che per l'oggetto e le informazioni in esso contenute non vi possano essere altre provenienze al di fuori di quella documentata*»; quello «*Processuale [che] scaturisce dalla necessità di garantire in qualsiasi fase dell'accertamento, a partire quindi dall'ambito nel quale ha origine il reperto, l'acquisizione e la perfetta gestione della fonte di prova scevra da qualsiasi pericolo di manipolazione o ipotesi di manipolazione che ne potrebbe diminuire il valore probatorio*».

[71] Si veda sul punto anche R. MURENEC, op. cit., pp. 128 e 129, dove viene fatto apposito rimando a quanto previsto da detta disposizione ai fini di garanzia dell'attendibilità e inalterabilità della prova informatica.

unicamente previsto che "*quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità…*".

Anche in questo caso la strategia del legislatore, stando alla terminologia adoperata, è lasciare la possibilità di fare ricorso alle *best practices* indicate dalle linee guida internazionali, senza imporre modalità attuative già predeterminate agli operatori.

Anche in questo caso però il ricorso alle migliori pratiche, stante l'omissione dell'indicazione di precise conseguenze in caso di violazione, non sembrerebbe comportare conseguenze sul piano della validità del reperto informatico.

Per la giurisprudenza, in particolare, la disposizione non imporrebbe modalità di custodia obbligatorie, contenendo direttive puramente indicative e di conseguenza derogabili sia per ragioni di assoluta impossibilità che di opportunità. Pertanto, scelte operative inidonee potrebbero avere effetto solo sotto il profilo della valutazione della prova *ex* art. 192 c.p.p., senza alcuna ripercussione nell'ottica della nullità o inutilizzabilità processuale del reperto digitale[72].

In buona sostanza, la giurisprudenza, ha riadattato le medesime conclusioni alle quali era già pervenuta in tema di acquisizione di *digital evidence*, sdoganando – anche nella fase della catena di custodia – il principio in base al quale il mancato rispetto di buone pratiche non costituisce automaticamente motivo di invalidità della prova informatica, potendo semmai costituire uno strumento per calibrare il peso giudiziario dell'elemento probatorio. È chiaro che in ogni caso, al fine di non incappare in un vizio motivazionale, il giudice in sentenza resta vincolato al dovere di evidenziare le motivazioni che lo hanno

[72] D. CURTOTTI, "Il sequestro", in "*Cyber forensics e indagini digitali Manuale tecnico-giuridico e casi pratici*", cit., p. 475, dove si legge: «*Si dica subito che le modalità di custodia delle cose sequestrate indicate dall'art. 260 costituiscono, per la giurisprudenza, prescrizioni meramente indicative che, da un lato, sono derogabili per ragioni di assoluta impossibilità o di opportunità, e, dall'altro lato, non sono astrattamente contestabili, tranne che nel caso in cui dalla loro mancata applicazione vogliano dedursi inconvenienti sostanziali attinenti a concrete ipotesi di alterazione, modificazione o sostituzione dei reperti. Ne consegue che l'inosservanza delle norme non è sanzionata da alcuna ipotesi di nullità ma può incidere unicamente sul diverso profilo della valutazione della genuinità della prova, secondo le regole generali dettate dall'art. 192 c.p.p.*».

addotto a prendere in considerazione elementi di prova provenienti da processi investigativi derogatori dei principi della catena di custodia.

Non vi è dubbio, comunque, che il rispetto delle indicazioni elaborate dagli standard internazionali fornisca un alto grado di attendibilità al reperto informatico, essendo pertanto detti principi, seppur non cogenti, diffusi nelle prassi operative. Ciò perché seguire tali principi per la custodia dei dati rende di fatto possibile, anche in momenti successivi, verificare l'autenticità del materiale informatico raccolto che potrà essere direttamente visionato, nonché pienamente conosciuto, sia dalle parti sia dal giudice stesso[73].

Dal punto di vista tecnico, nella *digital forensics*, la catena di custodia si concretizza consiste in un documento all'interno del quale viene riportata, oltre alla descrizione del reperto digitale, ciascuna operazione svolta in relazione al medesimo con l'indicazione del momento di svolgimento (data e ora) e del soggetto materialmente intervenuto. Altre informazioni possono riguardare gli spostamenti, il luogo di custodia e le modalità con la quale questa viene attuata[74].

In termini pratici, all'interno di tale documento viene descritto l'intero arco di vita della digital evidence nel contesto investigativo, dal momento della sua raccolta alla presentazione innanzi all'autorità giudiziaria[75].

[73] Si veda L. BARTOLI e C. MAIOLI, *"La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti"*, in Informatica e diritto, XLI annata, Vol. XXIV, 2015, n. 1-2, p. 141, dove trattando dell'importanza della trasparenza nella *digital forensics* e nella catena di custodia si precisa che *«Un'avvertenza preliminare sembra però opportuna: né le migliori tecniche né le più inespugnabili costruzioni normative possono eliminare in radice il pericolo di errori, perdite o incertezze. Alle norme spetterà il compito di salvaguardare, allora, non tanto la certezza dell'autenticità, quanto la trasparenza del percorso, l'occasione di conoscerne i passaggi. Per il giudice e le parti sarà così possibile smascherare i più malsicuri, considerarne il margine di rischio o ripercorrerli – a volte persino replicarli – così da corroborare o smentire la tenuta metodologica delle procedure adoperate»*. In proposito di tale affermazione, a loro volta gli autori operano un richiamo a E. CASEY, *"Digital Evidence and Computer Crime"*, III ed.,Waltham,Academic Press, 2011, p. 68 e ss.; ID., *"Error, Uncerainty and Loss in Digital Evidence"*, in International Journal of Digital Evidence, Vol. 1, 2002, p. 3, www.utica.edu

[74] Per un esempio grafico di documento di catena di custodia si veda R. MURENEC, op. cit., p. 129.

[75] *Ibidem,* dove in nota (269), facendo riferimento al modello di *chain of custody* dell'esperienza nordamericana, viene precisato che *«questo documento [la catena di custodia] deve sempre accompagnare, quasi fosse una "carta d'identità", gli elementi di prova, descrivendone in maniera precisa la res acquisita e indicando inequivocabilmente il nominativo degli individui che con essa entrano in contatto ed il momento e il luogo in cui ciò avviene».*

Per garantire il corretto funzionamento del meccanismo di conservazione è altresì necessario provvedere all'apposizione dei sigilli sia sul dispositivo originale, sia sui supporti contenenti le copie forensi[76].

Un'eventuale compromissione del sigillo potrà infatti rivelare una possibile manomissione dell'evidenza elettronica, con conseguente inattendibilità del materiale probatorio sul piano processuale.

La peculiarità della *digital forensics*, inoltre, impone di ragionare sul concetto di protezione dell'evidenza digitale da fattori esterni, con ciò intesi fenomeni provenienti da fonti estranee all'evidenza digitale e al supporto che la ospita ma capaci di influenzarne irrimediabilmente l'integrità e capaci di alterazioni da remoto, bypassando il sistema di sigillo fisico (pertanto molto complessi da individuare).

La questione della protezione della *digital evidence* dal pericolo di aggressioni ha ricevuto l'attenzione dei più importanti standard internazionali, tra i quali risalta l'ISO/IEC 27037:2012.

In particolare, le linee guida offerte da quest'ultimo si focalizzano sulla necessità di tutelare il dato informatico da fenomeni di perdita (*loss*), manomissioni (*tampering*) e distruzioni (spoliation) di informazioni, durante la fase di raccolta, trasporto e stoccaggio nel luogo finale di conservazione.

Infatti – prelevata la possibile prova dalla scena del crimine – occorre fare in modo che questa, una volta confezionata, giunga nel sito di deposito senza subire contaminazioni. È proprio un opportuno confezionamento o impacchettamento del materiale probatorio rinvenuto che scongiura quanto più possibile il prodursi di fenomeni deteriorativi, che possono provenire sia da condizioni naturali che da attività dolose o colpose (come ad esempio errori involontari degli operatori).

[76] Si veda D. CURTOTTI, ultima opera citata, p. 476, dove viene riportato un orientamento giurisprudenziale minoritario per il quale, usando le parole dell'autrice, «*risultano inutilizzabili le indagini condotte su un computer regolarmente sequestrato ma custodito in uno scatolone aperto, privo dell'apposizione di sigilli contrariamente a quanto dispone l'art. 260 c.p.p.*», la pronuncia n questione è Cass. Pen., Sez. III del 19 gennaio 2010.

Le cause di deterioramento naturale che possono colpire il dato digitale possono riguardare fenomeni ambientali (ad esempio l'umidità, che come risaputo danneggia i sistemi elettronici, fonti di calore oppure, qualora il reperto si trovi all'aperto, pioggia e condizioni atmosferiche in generale: dalla grandine che potrebbe colpire la componente hardware, ai fulmini che potrebbero mandare in *tilt* il sistema).

I fenomeni volontari, invece, possono consistere sia in danneggiamenti fisici prodotti direttamente sul supporto informatico sia in attacchi da remoto mediante accesso abusivo al sistema. Si pensi a dispositivi accesi con sistema *bluetooth* attivato, collegati ad altri dispositivi o direttamente connessi alla rete, dove qualsiasi utente in linea può rappresentare un rischio concreto di alterazione. Infine, occorre tenere presente l'alta sensibilità degli apparecchi elettronici nei confronti di campi elettromagnetici, onde radio e in generale frequenze generate da altri sistemi elettronici che potrebbero interferire irreversibilmente sull'integrità del dato, se non addirittura rendere inservibile il supporto dove è registrato.

Durante la fase di trasporto dell'evidenza digitale, pertanto, è necessario adottare strategie protettive utilizzando strumenti capaci di isolare il dispositivo prelevato dal mondo esterno, sia fisico che digitale.

Per i motivi sopra visti, infatti, non è sufficiente riporre l'elemento di prova informatico all'interno di comuni confezioni, come buste di carta o contenitori di plastica, utilizzati ad esempio per l'impacchettamento dei reperti biologici, ma sono necessarie tutele specifiche con l'ausilio di strumenti adeguati.

Tra le diverse soluzioni vi è l'inserimento del supporto prelevato all'interno di una gabbia di Faraday, ovvero un particolare contenitore composto da materiale elettricamente conduttore in grado di schermare le onde elettromagnetiche e le frequenze radio esterne, così rendendo impossibile l'interazione tra il dispositivo elettronico in esso contenuto e apparecchi o campi elettrostatici esterni[77].

[77]-Per un approfondimento sulla gabbia di Faraday e il suo impiego nell'informatica forense si veda il sito https://www.bit4law.com/blog/informatica-forense-incident-response/gabbia-di-faraday. Per esempi relativi a dispositivi utilizzabili per l'isolamento dei supporti informatici si veda https://www.dmi.unict.it/~battiato/CF1213.pdf dove vengono riportare in immagine alcune delle soluzioni adottabili.

Un altro strumento – per ovvi motivi di difficile impiego nella pratica – è il c.d. *jammer*, capace di inibire temporaneamente la funzione di emissione e ricezione delle onde radio degli apparecchi elettronici che si trovano all'interno del suo raggio d'azione, rendendo in questo modo impossibile comunicazioni tra questi e il supporto prelevato[78].

Simili strategie, chiaramente, devono essere adottate anche successivamente alla fase di trasporto e più propriamente all'interno del luogo di stoccaggio, dove oltre all'emarginazione del dispositivo dall'esterno potrebbero essere adoperati sistemi di videosorveglianza e sistemi altri accorgimenti per rendere inaccessibile a soggetti non autorizzati l'ingresso ai locali di custodia.

Nonostante tutti gli accorgimenti adottabili sul piano della sicurezza, preme sottolineare come il rischio di alterazione non sia mai completamente eliminabile[79]; talvolta, quindi, potrebbe rendersi necessario analizzare direttamente il supporto repertato per verificare che non vi siano state manomissioni o accessi da persone non autorizzate durante le fasi di raccolta, trasporto e conservazione.

In tali evenienze, procedere con dei controlli mirati si rivelerebbe quindi un utile strumento di garanzia ai fini dell'attendibilità del reperto, che – seppure trattato con la massima precauzione,– soggiace sempre, anche se in percentuali bassissime, al rischio di subire violazioni.

In particolare, a talune condizioni, con l'ausilio di appositi software è possibile ricostruire la timeline del dispositivo[80], per verificare che essa coincida con la sequenza cronologica di utilizzo come descritta nel documento della catena di custodia.

[78] Occorre precisare che l'uso di strumenti come il ***jammer***, proprio poiché volti ad azioni di disturbo delle frequenze radio e quindi ad impedire comunicazioni, è sottoposto a stringenti vincoli legislativi, si veda in proposito il dettato dell'art. 617 bis c.p. rubricato *«Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche»*.

[79] Come è risaputo nel campo della sicurezza informatica non esiste il c.d. "rischio 0", sussistendo sempre, nonostante le migliori cautele, una percentuale per quanto bassa di rischio.

[80] Per un approfondimento in tale senso si veda P. DAL CHECCO, *"Hacking-Boat 2019 – Digital Forensics"*, consultabile sul sito https://hackinboat.it/wp-content/uploads/2019/05/HackInBoat-Digital-Forensics-Paolo-Dal-Checco.pdf.

In estrema sintesi, nella *digital forensics* la catena di custodia costituisce un sistema procedurale che, seppure non obbligatorio sul piano giuridico, si rivela essenziale per il corretto esito delle indagini.

Il rispetto dei relativi principi e il corretto uso della strumentazione atta alla protezione del dato informatico, infatti, garantiscono la possibilità di condurre verifiche *ex post* sulla vita investigativa del reperto digitale.

Tutto ciò, nell'ottica del giusto processo, consente di consegnare nelle mani dei soggetti coinvolti nella dinamica giudiziale la possibilità di verificare in totale trasparenza l'integrità e l'autenticità del materiale probatorio.

Sul ruolo del gestore del sistema telematico nelle attività di *digital forensics*

Non di rado gli inquirenti, quando risulta necessario ricorrere alla *digital forensics*, si trovano a fronteggiare una serie di problematiche relative all'accesso al sistema informatico da analizzare. Oltre alle tecniche di anti forensics volte all'alterazione dei dati o semplicemente funzionali al rallentamento dell'attività investigativa, è frequente, infatti, che l'autorità procedente si trovi a dover operare su supporti e sistemi protetti da *password* o su informazioni oscurate mediante l'utilizzo di metodi crittografici[81] (c.d. *data hiding*).

Il problema che si pone per gli investigatori sta nel fatto che talvolta i sistemi di crittografia o di protezione potrebbero risultare particolarmente ostici da superare se non addirittura dannosi per l'indagine, come ad esempio può accadere nel caso in cui la crittografia includa sistemi di sicurezza informatica programmati alla cancellazione dei dati protetti o al blocco definitivo del dispositivo per il caso di tentativi di violazione, così implicando un elevato rischio di perdita del possibile elemento di prova.

Appare evidente come in dette situazioni il ricorso all'ausilio di privati esperti del settore o, ancora meglio, dello stesso gestore del sistema telematico attenzionato, possa apportare un contributo non indifferente per la buona riuscita dell'indagine. Il gestore, infatti, potrebbe essere a conoscenza delle debolezze del sistema e delle falle nella sicurezza, potendo talora, almeno in linea teorica, consegnare nelle mani dell'autorità procedente la chiave per l'accesso al dispositivo o comunque facilitare di molto le operazioni per "bucarne" le difese.

[81] Per crittografia s'intende quella «tecnica di rappresentazione di un messaggio in una forma tale che l'informazione in esso contenuta possa essere recepita solo dal destinatario; ciò si può ottenere con due diversi metodi: celando l'esistenza stessa del messaggio o sottoponendo il testo del messaggio a trasformazioni che lo rendano incomprensibile», https://www.treccani.it/enciclopedia/crittografia

In ragione di ciò occorre capire se i privati, tra i quali il gestore del sistema telematico, abbiano un dovere a collaborare alle indagini, oppure se possano rifiutarsi di prestare la loro cooperazione. In altri termini, bisogna comprendere se l'autorità procedente possa pretendere tale assistenza – obbligo che è stato definito da taluno *«servitù di giustizia»*[82] – oppure se il privato possa muovere opposizione a simile pretesa.

Partendo dal presupposto che è pacifico, nel nostro ordinamento, che tale pretesa non possa essere avanzata nei confronti dell'indagato e dell'imputato, stante il principio del nemo tenetur se detegere (inteso come il diritto a non dover compiere comportamenti autoincriminanti) ed è altrettanto pacifico che tale richiesta possa, invece, essere rivolta ai consulenti tecnici e privati obbligati a prestare la loro opera in base alle norme codicistiche[83], bisogna capire se tale obbligo sussista anche in capo al gestore del sistema telematico, il quale potrebbe trovarsi nella scomoda situazione di dover mettere a nudo le vulnerabilità del proprio sistema o peggio, a dover creare delle vulnerabilità *ad hoc* o rivelare stratagemmi capaci di eludere la propria sicurezza a soggetti che, sebbene membri delle forze dell'ordine o da questi delegati, sono comunque esterni all'azienda. Sotto altri punti di vista potrebbero profilarsi, poi, anche problemi collegati al diritto alla riservatezza, poiché fornire la chiave di crittografia di un sistema telematico, in linea teorica potrebbe rendere accessibile non solo il contenuto crittografato del dispositivo sotto indagine ma anche quello degli altri utenti che condividono la stessa struttura di crittografia.

In buona sostanza, giuridicamente parlando, si tratta quindi di stabilire fino a che punto l'esigenza di ordine pubblico possa spingersi nella compressione di diritti individuali a garanzia della sicurezza sociale, in tema di indagini informatiche[84].

Volgendo lo sguardo fuori dal nostro sistema giuridico, si deve rilevare come l'ipotesi per la quale l'esigenza investigativa possa scavalcare le ragioni del gestore informatico

[82] Tale locuzione è utilizzata in M. TORRE, op. cit., p. 1675 e pp. 1684 – 1685.

[83] Si veda ad esempio l'art. 359 c.p.p. in tema di accertamenti tecnici dove si precisa che i consulenti «*non possono rifiutare la loro opera*».

[84] La questione è posta in termini simili anche in M. TORRE, op. cit., pp. 1675 e ss.

è stata presa in considerazione anche presso altri paesi. Già da tempo, infatti, in diversi ordinamenti si è discusso sull'opportunità di imporre alle compagnie informatiche di progettare apposite *backdoors* ad uso investigativo, con ciò intese delle *«intenzionali vulnerabilità che l'autore del sistema dovrebbe introdurre nel proprio protocollo di crittografia, fornendone poi la chiave alla forza pubblica così da consentire di accedere, legalmente, ai dati cifrati a fine d'indagine e prevenzione di crimini particolarmente gravi»*[85].

In particolare è interessante osservare come la questione si sia posta in termini pressoché identici nell'ordinamento statunitense, dove sul punto si è sviluppato un nutrito dibattito andato alla ribalta con il caso giurisprudenziale che ha visto contrapposti il *Federal Bureau of Investigation* (F.B.I.) da una parte e il gigante informatico Apple Inc. dall'altra.

Il caso prendeva le mosse dall'indagine condotta dall'F.B.I. a seguito dell'attentato terroristico di matrice *jihadista* islamica passato alla cronaca come "la strage di San Bernardino", portato a segno nell'omonima località della California meridionale nell'autunno del 2015.

Stando all'accadimento dei fatti, durante l'attività investigativa gli inquirenti erano riusciti a rinvenire lo smartphone di uno degli attentatori e a porlo sotto sequestro per l'espletazione delle analisi di informatica forense. Tuttavia, il dispositivo risultava protetto da un complesso sistema crittografico volto alla difesa da accessi indebiti, che in caso di troppi errori nel tentativo di decifrazione avrebbe automaticamente (e definitivamente) cancellato le informazioni delle quali era posto a protezione[86].

[85] R. DE VITA e L. LAUDISA, *"Vita digitale a rischio: i captatori informatici tra pericoli per i diritti umani e riduzionismo giuridico"*, in Osservatorio CyberSecurity Eurispes, p. 3, articolo del 18 novembre 2019, consultabile sul sito https://www.devita.law/wp-content/uploads/2019/11/Vita-digitale-a-rischio.pdf.

[86] Nel particolare tecnico, il dispositivo recuperato dalla polizia «*risultava bloccato da un codice di blocco a 4 cifre e impostato per il wiping dei dati dopo 10 tentativi falliti nell'inserimento del codice di blocco, opzione presente nei dispositivi iPhone*», così F. MASSA, *"Il caso San Bernardino: APPLE vs FBI"* in sicurezzaegiustizia.com, consultabile sul sito https://www.sicurezzaegiustizia.com/il-caso-san-bernardino-apple-vs-fbi/. Quindi, il sistema di blocco consisteva in una strategia di sicurezza messa direttamente a disposizione dalla casa produttrice del congegno e non una struttura difensiva messa a punto dall'attentatore. È intuibile comprendere, dunque, come il gestore del sistema telematico avrebbe potuto aggirare le difese del dispositivo con relativa semplicità, o comunque apportare un contributo non indifferente al lavoro delle forze di polizia.

Vista la delicatezza della situazione, al fine di salvaguardare il contenuto digitale del dispositivo che avrebbe apportato un rilevante impulso per le indagini, i *detectives* dell'F.B.I. si appellavano direttamente alla multinazionale di tecnologia Apple Inc., in qualità di produttrice del modello di smartphone sequestrato e di responsabile del relativo sistema telematico, chiedendo a quest'ultima di prestare la propria collaborazione per lo sblocco del telefono.

Nello specifico veniva formulata richiesta nei confronti della società di creare e mettere nelle mani degli inquirenti un software apposito funzionale all'inibizione del sistema di distruzione dei dati, così da consentire alla pubblica autorità di poter eseguire in totale sicurezza tutti i tentativi che si sarebbero resi necessari per bypassare le difese del dispositivo.

La richiesta di cooperazione, tuttavia, veniva disattesa dalla società. Per il gigante informatico, infatti, la creazione di un programma finalizzato allo scopo voluto dagli investigatori, oltre a manifestarsi in palese contrasto con le politiche di riservatezza perseguite dalla società, se per qualsiasi motivo fosse finito nelle mani sbagliate avrebbe potuto mettere a rischio la privacy di tutti gli utenti in possesso del medesimo sistema.

Questo netto rifiuto finiva per costituire il presupposto per l'attivazione della disputa giudiziaria instaurata dall'F.B.I., rappresentata dal Dipartimento di Giustizia degli Stati Uniti, nei confronti della Apple Inc. Giudizio conclusosi con la dichiarazione di rinuncia alla prosecuzione dell'azione da parte del dipartimento della polizia federale, poiché nel frattempo, nonostante la mancata collaborazione, gli investigatori del *Federal Bureau of Investigation* erano ugualmente riusciti a superare le difese dello smartphone[87]. Ad ogni modo, pronunce più recenti vertenti su questioni analoghe hanno visto disattese le richieste della pubblica autorità in favore delle ragioni opposte dai responsabili dei sistemi informatici[88].

[87] Per una ricostruzione dettagliata della vicenda processuale in questione si rimanda a M. TORRE, op. cit., pp. 1678 e ss., qui preme osservare come un prima pronuncia sulla questione accoglieva le pretese del Dipartimento di Giustizia. Altri casi analoghi, invece, anche successivi alla vicenda riportata, hanno visto le richieste della forza pubblica disattese in favore delle ragioni dei gestori di sistemi telematici.

[88] *Ibidem*

Per quanto concerne il nostro ordinamento si deve precisare che precedenti plateali come quello appena analizzato, per il momento, non si sono ancora verificati; ciononostante la questione giuridica si propone ugualmente di attualità.

A differenza dell'esperienza statunitense, però, parrebbe che per il nostro assetto normativo l'interesse alla sicurezza collettiva debba essere considerato preponderante rispetto ai diritti dei singoli, fatta eccezione per una serie di situazioni giuridiche, tassative, che fanno da limite all'espansione del diritto alla sicurezza della collettività con conseguente riverbero in tema di repressione del crimine e quindi con effetti limitativi alla funzione investigativa: si pensi ad esempio alla centralità del diritto di difesa che impone il divieto di intercettare le conversazioni tra imputato e difensore, al diritto di non incriminarsi, alla tutela apprestata dalla legge al segreto professionale o, ancora, alle garanzie costituzionali relative alla dignità della persona[89].

Pertanto, al di fuori delle limitazioni espressamente previste dalla legge, è ben possibile che il gestore di un sistema telematico sia chiamato a prestare obbligatoriamente la propria assistenza alle forze dell'ordine anche nell'evenienza di indagini di *digital forensics*.

[89] Cfr. M. TORRE, op. cit., p. 1685.

White Paper

SAFETY & SECURITY MANAGER

Download gratuito su www.safetysecuritymagazine.com

Attività di *digital forensics* e diritto di difesa

Se da un lato la potenzialità investigativa offerta dalle nuove tecniche dell'informatica forense comporta un indiscutibile vantaggio per il lavoro degli inquirenti, dall'altro, se non debitamente perimetrata all'interno di una disciplina ben delineata, rischia inevitabilmente di porre a rischio le garanzie con le quali la Costituzione ha inteso tutelare il diritto di difesa e il giusto processo (artt. 24 e 111 Cost.).

La fragilità che contrassegna la *digital evidence*, infatti, rende le attività di digital forensics estremamente delicate e una scarsa attenzione normativa (oppure orientamenti giurisprudenziali più attenti alle necessità di repressione dei reati che alle garanzie difensive), potrebbero aggravare non di poco la posizione del soggetto sottoposto alla macchina processuale.

La lacunosità della disciplina codicistica – che, come visto, si limita a richiedere l'adozione di modalità idonee alla salvaguardia del dato – unita alla posizione della giurisprudenza dominante che sembrerebbe abbracciare soluzioni poco inclini a considerare necessaria la partecipazione dell'indagato nel momento acquisitivo, lascia intendere che il tentativo di contemperazione tra esigenze investigative ed esigenze difensive tenda, nel nostro ordinamento, a privilegiare le prime.

È proprio l'insufficienza del contraddittorio che contraddistingue la fase di acquisizione in copia forense, giudicata atto ripetibile e pertanto eseguibile autonomamente dall'autorità procedente in assenza della controparte giudiziale, che però riduce notevolmente il principio di dialettica tra le parti che il nostro modello processuale (prevalentemente accusatorio) ha fatto proprio, con conseguente smussamento dell'"arsenale difensivo" a disposizione dell'indagato. Se si tiene inoltre conto del fatto che un certo grado di disparità sussiste in ogni caso, anche nel corso delle indagini tradizionali, si può cogliere

come la sperequazione tra accusa e difesa sia destinata ad aumentare in caso di attività di *digital forensics*.

Ora, se è vero come sostiene la giurisprudenza che l'estrazione in copia forense costituisce una mera operazione meccanica, è anche vero che la volubilità del dato consente di affermare che si tratti comunque di un tipo di attività altamente aleatoria e che anche il minimo errore potrebbe condurre ad esito fatale per il processo e per l'accusato. Ad esempio, uno scorretto uso delle apparecchiature, una piccola disattenzione o anche fattori ambientali potrebbero comportare alterazioni involontarie come la cancellazione di dati idonei a dimostrare che in un determinato momento l'indagato stava utilizzando il computer e dunque non poteva trovarsi altrove a commettere il reato.

Al contrario, immedesimandosi negli investigatori, talvolta anticipare il contraddittorio alla fase acquisitiva potrebbe significare dover anticipare la *discovery* del materiale probatorio ad una fase ancora acerba; con conseguente rischio di mettere in allerta un eventuale colpevole che potrebbe così riuscire a correre ai ripari, anche se in realtà tale evenienza non sembra essere sufficiente a giustificare la limitazione del principio costituzionale del diritto alla difesa.

Altra situazione è quella in cui l'eventualità del caso concreto non consente all'autorità procedente di poter dilazionare le operazioni ad altro momento in attesa dell'instaurazione del contraddittorio, poiché la situazione impone di agire con assoluta urgenza.

Una soluzione capace di rappresentare un punto di incontro tra necessità investigative e garanzie difensive potrebbe essere quella – già enucleata da parte della dottrina attiva nel settore delle scienze forensi – di affiancare all'operatore incaricato dall'autorità un esperto, inteso come *«consulente tecnico a futura memoria»*[90], che avrebbe il ruolo di par-

[90] N. FUSARO, "*Delitti e condanne… Prova scientifica e ragionevole dubbio*", in Osservatorio del Processo Penale, 2009, pp. 4-5. Lo stesso concetto viene riportato dal medesimo autore anche nell'opera *"La sentenza assolutoria della Corte di assise d'appello di Perugia per l'omicidio di Meredith Kercher, tra valutazione della prova scientifica e prevalenza del principio dell'oltre ogni ragionevole dubbio. L'analisi del criminologo"*, in *"L'assassino di Meredith Kercher"*, Aracne, 2012, p. 379, dove si legge *«soprattutto nelle prime fasi di indagine, durante il sopralluogo e nel corso degli altri atti irripetibili, quale l'autopsia, appare opportuna, essendo nella quasi totalità dei casi ancora ignoto l'autore del reato, la già richiamata previsione di un consulente difensivo "a futura memoria", che vesta anche solo e semplicemente le vesti di discussent, garantendo anticipatamente quella dialettica che, pur prevista dal nostro codice di procedura all'art. 358 c.p.p., finisce il più delle volte per essere totalmente disattesa».*

tecipare alle operazioni di acquisizione o anche solo di supervisionarle ed eventualmente intervenire consigliando le migliori modalità tecniche, così da poter in qualche modo anticipare il contraddittorio tra le parti anche nelle occasioni in cui l'indagato non possa partecipare. Inoltre, una simile figura infonderebbe sicuramente un grado di attendibilità maggiore al materiale informatico estratto. È ovvio, in ogni caso, che questa soluzione dovrebbe essere considerata pur sempre secondaria rispetto alla possibilità di intervento del diretto interessato o di esperti da quest'ultimo nominati.

L'importanza dell'intervento di un esperto nella veste di "consulente tecnico a futura memoria", che controlli la fase di acquisizione in ottica di tutela preventiva dell'indagato, potrebbe essere avvertita come essenziale se si tiene conto degli arrivi giurisprudenziali per i quali è stato giudicato non obbligatorio, ai fini dell'utilizzabilità del materiale informatico, l'aver seguito i criteri operativi messi a punto dalle *best practices*.

Proprio la non obbligatorietà del rispetto delle migliori pratiche, intesa come utilizzabilità della digital evidence ottenuta con procedimenti non riconosciuti dagli standard internazionali, si rivela un'altra causa di aggravio nei confronti dell'indagato. Come stabilito dalle già esaminate sentenze pronunciate nel caso Vierika, in base ad un meccanismo di inversione dell'onere probatorio diventa, infatti, compito della difesa trovare elementi capaci di destituire l'attività svolta dagli inquirenti, che nella loro funzione sono liberi di discostarsi dalle regole precostituite dai protocolli comunemente riconosciuti senza inciampare in ipotesi di invalidità. In pratica, l'indagato si ritrova nella situazione di dover dimostrare da un lato l'avvenuta violazione delle *best practices* e, dall'altro, che tale violazione abbia prodotto un possibile pregiudizio all'integrità del dato digitale raccolto. È superfluo precisare come il riuscire a provare l'inattendibilità del materiale probatorio senza aver avuto la possibilità di partecipare all'acquisizione del medesimo si traduce a tutti gli effetti in un'ipotesi di *probatio diabolica*.

Sul punto occorre richiamare un moderno orientamento per il quale l'onere probatorio dovrebbe cadere sull'accusa e verrebbe correttamente assolto qualora fossero indicate talune circostanze, ovvero: il soggetto che ha individuato il dato informatico, come il dato si presentava al momento del rinvenimento, modo e tempo di acquisizione del dato e modalità di successiva conservazione[91]. Spetterebbe poi alla difesa, in ottica di ripartizione

dell'onere probatorio, riuscire a dimostrare anche sul presupposto di proprie attività investigative la non genuinità del reperto[92].

Si deve osservare, tuttavia, come anche seguendo tale approccio, sebbene più rispettoso delle esigenze difensive, non si riuscirebbe comunque ad attenuare del tutto il carattere diabolico della prova contraria che l'indagato dovrebbe individuare per smantellare la tesi dell'accusa. Le indicazioni che dovrebbero integrare il valore probatorio del dato digitale, infatti, sarebbero in ogni caso faticosamente confutabili da una parte processuale che non ha avuto la possibilità materiale di partecipare alle attività investigative che hanno riguardato quel dato.

In pratica, anche se si volesse appoggiare questo nuovo orientamento, non vi è dubbio che in caso di eventuali incertezze queste graverebbero, inevitabilmente, sulla posizione dell'indagato contro il quale la prova è utilizzata. Situazione che fuoriesce dagli schemi del processo prevalentemente accusatorio del codice del 1988, assumendo un tono squisitamente inquisitorio.

La posizione subalterna dei diritti dell'indagato rispetto all'esigenza investigativa, in ultimo, si riflette anche sul diritto alla riservatezza. Le operazioni di *digital forensics*, infatti, si manifestano come attività particolarmente invasive dal punto di vista della riservatezza, concretizzandosi in un'intrusione non irrilevante nella sfera privata del soggetto indagato. Questo perché computer, smartphone e simili, oltre a contenere i possibili elementi di prova ricercati, immancabilmente fanno da contenitore ad una grande quantità di informazioni e dati sensibili che nulla hanno a che fare con il presunto delitto. Metaforicamente parlando, nella società odierna tali dispositivi sono a tutti gli effetti equiparabili a delle vere e proprie casseforti digitali di dati personali, che con questo tipo di operazioni vengono inevitabilmente forzate. Partendo da tale presupposto, appare opportuno comprendere fino a che punto gli inquirenti possano spingersi nel trattare reperti informatici.

In sostanza appare opportuno chiedersi se – e come – la portata invasiva delle moderne tecniche dell'informatica forense possa essere limitata in favore al diritto alla privacy

[91] R. MURENEC, op. cit., p. 114.

[92] *Ibidem*

dell'indagato. Invero, il legislatore e la giurisprudenza nell'ultimo decennio hanno già avuto modo di confrontarsi con il tema della capacità invasiva delle nuove tecnologie, peraltro in materie che per molti aspetti possono paragonarsi, dal punto di vista privacy, alla *digital forensics*. Tra queste, prima fra tutte la recente disciplina relativa alle intercettazioni ambientali a mezzo captatore informatico, ossia quel tipo di intercettazioni condotte con l'uso di un *«un software (rectius: malware) di tipo trojan che si introduce occultamente nelle "mura protette" di un sistema informatico»*[93] e che una volta al suo interno è in grado di monitorarlo e potenzialmente di esfiltrarne, da remoto e di nascosto, il contenuto digitale.

Ebbene, la normativa del captatore – e delle intercettazioni in generale – proprio in considerazione della sua capacità penetrativa nella vita dell'indagato, seppure con qualche incertezza, ha limitato la possibilità del suo utilizzo solo ad alcuni tipi di reato e solo al ricorrere di determinate condizioni[94].

Sul punto è sufficiente osservare che, anche in materia di *digital forensics*, non vi è motivo di non ritenere che una limitazione alla possibilità di ricorso alle operazioni di acquisizione in copia forense solo per fatti di reato in grado di arrecare un particolare disvalore sociale, potrebbe essere un giusto contemperamento tra necessità investigative e tutela della riservatezza dell'indagato.

Ad ogni modo, seppure un contemperamento tra dovere di repressione dei reati e privacy in tema di digital forensics, nei termini visti, al momento ancora non è stato oggetto di dibattito, occorre prendere nota di una recente pronuncia giurisprudenziale, scaturita da un

[93] O. CALAVITA, "L'odissea del trojan horse, Tra potenzialità tecniche e lacune normative", in Diritto Penale Contemporaneo, fasc. 11/2018, p. 46.

[94] Si consideri che la disciplina vigente in materia di captatore informatico ne legifera l'utilizzo unicamente in materia di intercettazioni ambientali. Attualmente il "trojan di stato" può essere usato esclusivamente per i reati contemplati dall'art. 266 c.p.p. e ne è proibito l'uso all'interno dei luoghi indicati dall'art. 614 c.p., salvo che vi sia fondato motivo di ritenere che ivi si stia svolgendo l'azione criminosa. Limitazione che tuttavia non si applica per i procedimenti di criminalità organizzata di stampo mafioso e terrorismo e, previa indicazione delle ragioni giustificative, anche per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione con pena della reclusione non inferiore nel massimo a cinque anni.

caso di notevole impatto mediatico, relativo a fatti di finanziamento illecito a partiti politici e traffico di influenze illecite, con la quale la Suprema Corte, tenuta in considerazione l'eventualità che nelle indagini informatiche vengano acquisite informazioni "*sensibili*" o "*supersensibili*", ha evidenziato le modalità operative e i limiti ai quali deve soggiacere il sequestro probatorio di dati informatici e telematici[95].

In particolare, ribadendo il principio del divieto di esecuzione di indagini meramente esplorative, la Cassazione ha precisato che in caso di sequestro attraverso apprensione fisica delle memorie di sistemi elettronici, una volta realizzata una copia integrale del contenuto del sistema (denominata *«copia mezzo»*) questa debba essere analizzata al fine di selezionare i contenuti pertinenti al reato per cui si procede e quindi restituita al legittimo titolare, giacché la medesima, una volta carpiti gli elementi utili alle indagini, non rileva di per sé quale cosa pertinente al reato, trattandosi unicamente di *«un insieme di dati indistinti e magmatici»*. In sintesi, la copia integrale va intesa come un mero strumento dal quale reperire le informazioni pertinenti al reato e in conseguenza di ciò, non sussistendo reali ragioni al trattenimento di qualsiasi altro tipo di dato in essa contenuto, può essere trattenuta esclusivamente per il tempo strettamente necessario all'espletamento delle operazioni di selezione del materiale di interesse investigativo[96].

[95] Cass. Pen., Sez. IV, Sent. n. 34256 del 2020

[96] Sull'argomento si veda M. Pittiruti, *"Dalla Corte di Cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus"*, in Sistema Penale, consultabile sul sito https://www.sistemapenale.it/it/scheda/cass-sez-vi-sent-22-settembre-2020-dep-2-dicembre-2020-n-34265-pres-di-stefano-rel-silvestri

Precedenti emblematici: il caso Mered e la sentenza di primo grado sul caso di Garlasco

Al pari delle altre prove scientifiche, la *digital evidence* esige di essere trattata con estrema cura e valutata con particolare attenzione. Il fatto che l'elemento probatorio sia il frutto di un procedimento scientifico non significa di per sé che sia sicuramente attendibile; o meglio, sebbene scientificamente attendibile, non dimostra automaticamente che un soggetto abbia realizzato una determinata condotta criminosa. Per fare un esempio, il rinvenimento di una traccia genetica in un luogo non vuol dire conseguenzialmente che il soggetto che l'ha lasciata abbia commesso il delitto ivi consumato. Costui potrebbe essere passato in quel luogo in un momento precedente o successivo, oppure la traccia genetica potrebbe esservi stata trasportata involontariamente da altri soggetti sui quali, per qualsiasi ragione, si era posata. Da questo esempio si comprende agevolmente il fattore da tenere sempre in considerazione quando ci si trova a trattare la prova scientifica, ovvero la contestualizzazione del reperto rinvenuto.

Ne deriva che anche il dato digitale estratto mediante acquisizione in copia forense vada valutato e contestualizzato all'interno dell'intero quadro investigativo, tenendo a mente che da un'errata analisi potrebbe scaturire un'erronea interpretazione del quadro probatorio nel suo complesso e, di conseguenza, un errore giudiziario.

Tra i casi giudiziari più recenti dove una scorretta interpretazione degli esiti delle operazioni di informatica forense ha rischiato di trasformarsi in un clamoroso errore giudiziario vi è il processo celebratosi presso la Corte d'Assise del Tribunale di Palermo nei confronti del cittadino eritreo Behre Medhanie Tasmafarian, noto alla cronaca giudiziaria come caso Mered[97].

[97] Corte d'Assise del Tribunale di Palermo, Sent. del 12 luglio 2019.

Una serie di errori investigativi avevano convinto le autorità britanniche a ritenere che Behre Medhanie Tasmafarian fosse in realtà il trafficante di migranti Medhanie Yehdego Mered detto "il generale", ricercato dalle forze dell'ordine di diversi paesi.

Le errate intuizioni portavano nel 2016 all'arresto del cittadino eritreo mentre si trovava in Sudan e successivamente alla sua consegna mediante estradizione in Italia, dove veniva posto sotto custodia cautelare in carcere e quindi processato con l'accusa di tratta di esseri umani.

Le inesattezze investigative originavano dall'interpretazione di alcune frasi pronunciate dal Bhere, mentre comunicava col proprio telefono cellulare, parlando di viaggi migratori. Questa circostanza, unita all'omonimia tra il cittadino eritreo e il generale, induceva le forze britanniche ad inciampare nella convinzione che si trattasse della stessa persona. Seguiva il sequestro del dispositivo e la sua sottoposizione alla procedura di estrazione in copia forense, mediante la quale venivano clonate tutte le chat presenti sul dispositivo – quelle presenti sui social network comprese – tutti i file audio, video, immagine, i dati di navigazione internet e tutta la cronologia delle telefonate effettuate, sia tramite applicazione che sulla linea telefonica tradizionale[98]. Tuttavia, ancora una volta, i dati estratti venivano fraintesi non facendo altro che avvalorare l'erronea tesi propugnata dall'accusa, in seguito smontata unicamente grazie alla prova genetica e agli esiti della perizia fonica che accertavano come si fosse trattato, in realtà, di soggetti diversi. Seguiva quindi, dopo tre anni di carcerazione preventiva, la sentenza assolutoria con la quale il Tribunale di Palermo stabiliva il non doversi procedere dopo aver accertato l'avvenuto scambio d'identità tra il cittadino eritreo coinvolto nel processo e il trafficante di migranti Medhanie Yehdego Mered.

Un altro caso emblematico, dove la *digital forensics* ha giocato un ruolo fondamentale, è il celebre "delitto di Garlasco", relativo al tragico omicidi o di una giovane ragazza nell'omonima località della provincia pavese e dal quale è scaturito uno dei processi mediatici

[98] Sulla questione si veda l'inchiesta dalla testata giornalistica online Irpimedia, *"Errori giudiziari: come la prova tecnologica manda in carcere un innocente"* realizzata ad opera di R. COLUCCINI, consultabile sul sito https://irpimedia.irpi.eu/prova-tecnologica-caso-mered/.

più seguiti dalla cronaca giudiziaria italiana.

Senza entrare nel merito della vicenda processuale, durata ben cinque gradi di giudizio con due pronunce della Suprema Corte e conclusasi con la condanna definitiva del fidanzato della vittima, è di interesse la pronuncia assolutoria di primo grado emessa dal Tribunale di Vigevano[99], dove sono stati effettuati ampi ragionamenti in merito al valore attribuibile ad una prova informatica colpita da fenomeni contaminativi[100].

Nel caso di specie, il reperto informatico attenzionato durante le indagini consisteva nel personal computer dell'imputato, utile al fine di stabilire l'attendibilità dell'alibi del medesimo durante la mattina in cui si era svolta l'azione delittuosa. Secondo la ricostruzione dell'imputato, infatti, durante i momenti in cui si consumava l'omicidio egli si sarebbe trovato nella propria abitazione, innanzi al proprio computer, intento a lavorare alla tesi di laurea.

L'analisi del dispositivo, una volta accertato che per motivi tecnici non sarebbe stato possibile un suo utilizzo sulla scena del crimine, si palesava dunque necessaria al fine della ricostruzione della timeline delle attività ivi compiute, al fine di stabilire se il dispositivo fosse stato realmente adoperato in orari compatibili con quelli dell'omicidio.

Si poneva, tuttavia, un problema di non poco conto: durante le prime fasi d'indagine la genuinità delle informazioni memorizzate nel computer era stata pesantemente compromessa. Come riportato in sentenza, *«quando il reperto informatico veniva consegnato ai consulenti tecnici del pubblico ministero che procedevano all'effettuazione delle copie forensi dello stesso, i carabinieri accedevano ripetutamente e scorrettamente (senza l'utilizzo, cioè delle necessarie tecniche forensi di indagine) alla quasi totalità del contenuto del computer»*[101].

[100] Sullo stesso argomento si veda anche A. GAMMAROTA con relatore C. MAIOLI, *"Informatica forense e processo penale: la prova digitale tra innovazione normativa e incertezze giurisprudenziali"* [dissertation thesis], 2016, pp. 120 e ss., consultabile sul sito http://amsdottorato.unibo.it/7723/1/Gammarota_Antonio_tesi.pdf, opera dalla quale si sono prese le mosse per la disamina della questione.

[101] Nel particolare le operazioni scorrette svolte dai carabinieri che per primi accedevano al dispositivo erano consistite in *«sette (e non cinque come riferito) accessi al personal computer di Alberto Stasi; non corretta indicazione dell'avvenuta installazione ed utilizzo di diverse periferiche USB (oltre a quella correttamente indicata); non corretta indicazione dell'avvenuto accesso al disco esterno in uso ad Alberto Stasi; non corretta indicazione di accessi multipli al file della tesi di laurea in vari percorsi di memorizzazione dello stesso: si vedano sul punto i rilievi del collegio peritale tecnico/informatico».*

L'effettuazione di tali accessi, condotti senza il rispetto dei principi basilari dell'informatica forense già noti all'epoca delle indagini[102], provocava *«la sottrazione di contenuto informativo con riferimento al personal computer di Alberto Stasi pari al 73,8% dei files visibili (oltre 56.000) con riscontrati accessi su oltre 39.000 files, interventi di accesso su oltre 1500 files e creazione di oltre 500 files. Insomma interventi che hanno prodotto effetti devastanti in rapporto all'integrità complessiva dei supporti informatici (in questi termini si esprime il collegio peritale)»*, come si legge in un passaggio successivo *«Si deve, dunque, ritenere che questa preliminare e sommaria attività investigativa è stata posta in essere secondo una metodologia sicuramente scorretta, disattendendo i protocolli già invalsi in materia (anche prima dell'entrata in vigore della legge citata) venendo, quindi, a costituire una causa di potenziale alterazione e dispersione del contenuto del documento informatico»*.

Alla luce dei danni arrecati al contenuto digitale del dispositivo, descritti come *«devastanti»*, il giudice si trovava dunque innanzi alla necessità di comprendere se le informazioni in esso ricavabili potessero essere ugualmente utilizzabili in giudizio – e in caso positivo fino a che punto – oppure se, a prescindere, si fosse dovuta dichiararne l'inutilizzabilità.

Partendo dall'assunto che, nonostante gli accessi incauti dei primi investigatori, i consulenti dell'accusa riuscirono ugualmente a stabilire, con le immancabili incertezze del caso, una *timeline* delle operazioni del dispositivo[103], in sentenza non è stata adottata una po-

[102] Sul punto si deve tenere presente che, sebbene la sentenza risalga alla fine del 2009, le attività di indagine sul dispositivo si sono svolte in un periodo di poco successivo alla commissione del delitto, risalente all'estate del 2007, momento in cui la legge n. 48 del 2008 ancora non era entrata a far parte del nostro ordinamento. Tuttavia, la pronunci mette in chiaro come, nonostante la legge sia entrata in vigore in un momento successivo alle indagini, le metodologie tecniche proprie della *digital forensics* erano già invalse nella prassi delle attività investigative aventi ad oggetto reperti informatici.

[103] Più precisamente in sentenza si legge: *«Il complesso di queste alterazioni veniva rilevato anche dai consulenti tecnici del pubblico ministero (i Ris di Parma) nella loro successiva analisi. Pur tenendo conto di quanto sopra, i Ris, nella loro relazione tecnica e successive integrazioni e chiarimenti, concludevano sostanzialmente nel senso che il giorno 13 agosto 2007 il computer portatile di Alberto Stasi veniva acceso alle ore 9.36; quindi venivano aperte delle fotografie digitali fino alle ore 9.57 e dopo le ore 10.17 non sarebbero presenti tracce informatiche che comportino la presenza attiva di un utente che interagisce con il PC», tuttavia, il collegio peritale, sempre come indicato in sentenza, riusciva in ogni caso mediante l'estrazione dei metadati esterni al sistema operativo a stabilire «con certezza (e questo è un'evidenza probatoria non contestata dalle parti) l'interazione diretta e sostanzialmente continuativa dell'utente con il computer dalle ore 10.17 fino alle ore 12.20 del giorno 13 agosto».*

sizione di assoluto rifiuto nei confronti della prova informatica acquisita con le modalità sopra viste.

Il giudice, nel percorso logico che lo ha condotto alla decisione, ha operato una verifica degli elementi informatici incrociandoli con dati estratti da altri dispositivi elettronici. Sostanzialmente, l'attendibilità delle *digital evidence* estratte dal computer dell'imputato non è stata cercata unicamente all'interno delle stesse, bensì si è fatto ricorso ad elementi esterni ad esse per valutare se e in che modo tutte le risultanze, ad un esame incrociato, combaciassero tra loro.

In altre parole è stato fornito un giudizio di attendibilità della prova informatica, con conseguente conferma positiva circa la sua utilizzabilità processuale, ricorrendo ad altri elementi che in qualche modo, secondo il giudice, hanno consentito di dare conferma della genuinità delle informazioni estratte dal computer dell'imputato per quanto riguarda la linea temporale delle operazioni svolte .

Benché l'aver giudicato utilizzabile del materiale ottenuto con metodologie di acclarata scorrettezza procedurale desti sicuramente delle perplessità, si deve osservare come in ogni caso la pronuncia abbia il merito di aver chiarito come metodi investigativi non conformi alle logiche scientifiche possano comportare, nelle procedure di digital forensics, danni irreparabili alle evidenze informatiche, le quali, peraltro, necessitano di essere calate all'interno dell'intero quadro dell'indagine e non valutate in autonomia[104].

[104] Si veda A. GAMMAROTA, op. cit., pp. 136-138 dove, nonostante la sentenza sia ormai risalente nel tempo, si ritiene che *«il percorso logico-argomentativo della sentenza appena ripercorsa si pone come moderno paradigma per la corretta valutazione dell'attendibilità dei dati, nonché della corretta interrelazione delle informazioni derivanti dai dispositivi digitali».*

White Paper “Quaderni di Cyber Intelligence” #1

CYBER INTELLIGENCE

Download gratuito su www.ictsecuritymagazine.com

Digital forensics e *cyber security*: caso Cellebrite Ufed v. Signal

Dal punto di vista tecnico-operativo, le indagini di digital forensics vengono svolte utilizzando specifici strumenti hardware e software[105] che, una volta collegati al sistema informatico da acquisire, ne esplorano le aree di memoria e ne producono una copia[106] – nella quale vengono ricompresi lo spazio non allocato e le parti di file cancellati ma non definitivamente eliminati – che successivamente viene esfiltrata verso un file di *backup* appositamente creato sul dispositivo hardware usato per l'acquisizione e dove viene, quindi, dislocata la copia forense del sistema sotto indagine. Concluse le operazioni di acquisizione, il clone informatico viene poi analizzato mediante programmi di analisi che permettono di prendere visione del contenuto digitale in esame. In particolare, questi software hanno il compito di scandagliare a fondo tutti i singoli file che sono presenti nella copia forense, visionandone tutte le parti, metadati inclusi, verificando che non vi siano contenuti occultati e nel caso procedendo ad analisi dei medesimi[107].

È ovvio che più il programma di analisi è moderno e aggiornato più sarà in grado di scovare file nascosti e di conseguenza maggiore sarà la resa in termini di risultato finale.

Qualora, invece, i file siano protetti da password, occorrerà procedere allo sblocco del loro contenuto mediante attacchi brute force volti all'individuazione della chiave che cu-

[105] Per un approfondimento delle diverse tipologie di software che vengono utilizzati nelle operazioni di informatica forense e sul funzionamento degli stessi si rimanda a M. VITIELLO, *"Il laboratorio di informatica forense: i software, gli strumenti hardware, i costi"* consultabile sul sito https://www.agendadigitale.eu/documenti/il-laboratorio-di-informatica-forense-i-software-gli-strumenti-hardware-i-costi.

[106] Si rammenta che per impedire che i dati da acquisire vengano corrotti dallo strumento di acquisizione medesimo è necessario che questo abbia la funzione di blocco di scrittura (*write blocking*).

[107] Per recuperare file cancellati oppure danneggiati vengono impiegati appositi strumenti di file recovery che servono proprio a ripristinare contenuti parziali.

stodisce i dati[108].

In estrema sintesi e senza tecnicismi, l'attività di individuazione della *digital evidence* è suddivisibile in due fasi: la prima è quella di acquisizione in copia forense della memoria del dispositivo, mentre la seconda prevede l'analisi della copia estratta, fase nella quale, più precisamente, vengono rintracciate e identificate le evidenze digitali stoccate in memoria che si sospettavano poter essere presenti sul dispositivo al momento del sequestro.

Per entrambe le fasi, in situazioni particolari, possono profilarsi problemi di sicurezza informatica. Durante tali momenti, ad esempio, delle criticità potrebbero insorgere qualora il dispositivo da acquisire e analizzare sia infetto da un virus informatico. Clonando la memoria inevitabilmente verrebbe clonato anche il programma malevolo, che per conseguenza si estenderebbe alla copia forense.

Ora, se l'infezione sul dispositivo originario fosse nota, il problema in realtà non si porrebbe. In tal caso, infatti, l'ostacolo potrebbe essere facilmente aggirato acquisendo più copie del dispositivo e quindi procedendo alla disinfezione del virus da una di esse, per poi confrontarla con le altre per valutare se l'operazione di eliminazione del malware abbia comportato la compromissione di dati oppure abbia mantenuto inalterate le informazioni[109].

Il problema emerge quando il virus informatico passa inosservato all'occhio dei software adoperati per le operazioni forensi. Si consideri sul punto che, al pari degli altri programmi informatici, anche gli strumenti adoperati per la *digital forensics* possono avere delle vulnerabilità nella sicurezza, soprattutto quando il sistema non viene regolarmente ag-

[108] L'attacco di brute force «*consiste nel provare tutte le possibili combinazioni di lettere, caratteri speciali e numeri finché non individua la mescolanza giusta. Un'operazione che viene, ovviamente, eseguita da un software. Il tempo di riuscita dell'impresa dipende dalla velocità di calcolo del computer, nonché dalla complessità e la lunghezza della password (quanti e quali caratteri sono stati utilizzati)*». La definizione è tratta da R. RIJITANO, *"Brute force: cosa sono, come fare e prevenire gli attacchi a forza bruta"*, consultabile sul sito https://www.cybersecurity360.it/nuove-minacce/brute-force-cosa-sono-gli-attacchi-a-forza-bruta-come-farli-e-prevenirli/.

[109] Ovviamente, in ogni caso, in sede processuale bisognerà capire se e in che modo il programma malevolo possa aver corrotto le informazioni sulla copia originale prima che venisse rilevato.

giornato. In linea teorica, pertanto, potrebbe capitare che un malware sfugga al controllo e continui a svolgere indisturbato il compito per il quale è stato progettato.

In particolare, esistono alcuni tipi di malware che una volta sottoposti all'azione dei programmi di analisi sono in grado di corromperne l'algoritmo e alterarne il funzionamento per far commettere al software operazioni per le quali originariamente non era settato o che non era stato autorizzato a svolgere. È superfluo specificare che in simili evenienze l'attendibilità delle risultanze ottenute con l'analisi forense sarebbe del tutto assente.

Ad ogni modo, vulnerabilità di questo tipo non colpirebbero la genuinità del procedimento di formazione della copia forense, ma esclusivamente il successivo passaggio di analisi, compromettendo quindi non l'acquisizione in sé (consistente in una mera copiatura dei byte della memoria originale senza attività di elaborazione) ma solo i sistemi di analisi e in conseguenza l'analisi che ne scaturisce[110].

Un recente caso di cronaca, andato alla ribalta delle testate giornalistiche che si occupano di cybersicurezza, ha messo in chiaro come quanto appena descritto non sia solo un'ipotesi di scuola, bensì potrebbe realmente accadere, o meglio, sarebbe già accaduto. Il caso riguarda lo scambio di battute avutosi tra fine 2020 e prima metà del 2021 tra la nota app di messaggistica Signal e l'azienda israeliana produttrice di strumenti di informatica forense – tra le più affermate sul mercato – Cellebrite Ufed.

La disputa aveva origine allorché l'azienda israeliana comunicava pubblicamente di aver trovato il modo per violare le difese dell'applicazione di messaggistica – come noto tra le più sicure e tra le più improntate alla garanzia della privacy degli utenti – affermando di esserne persino riuscita decifrare i contenuti delle chat e i relativi allegati. Successivamente, sebbene l'azienda, sul presupposto delle polemiche che stavano emergendo, avesse tentato di ridimensionare la portata sensazionalistica della comunicazione originale, si scatenava ugualmente la reazione di Signal.

[110]-Quanto finora riferito e la disamina che segue trae le mosse da P. DAL CHECCO, *"Signal ha hackerato Cellebrite, svelate vulnerabilità nelle app di hacking telefonico: i risvolti"*, in Cybersecurity360 consultabile sul sito https://www.cybersecurity360.it/nuove-minacce/signal-ha-hackerato-cellebrite-svelate-vulnerabilita-nelle-app-di-hacking-telefonico-i-risvolti/.

Per tutta risposta infatti quest'ultima, a mezzo di un articolo pubblicato pochi mesi dopo dal proprio amministratore delegato[111], nello sminuire ulteriormente la notizia dell'hackeraggio[112] controbatteva insinuando di essere stata a sua volta in grado di individuare alcune vulnerabilità presenti sul software di analisi Physical Analyzer, sviluppato e distribuito sul mercato dalla società israeliana.

In pratica, secondo l'amministratore delegato di Signal, il software della Cellebrite dopo il lancio nel 2012 non sarebbe più stato implementato con i necessari aggiornamenti, sicché avrebbe presentato diverse falle nel proprio sistema di sicurezza. Sfruttando queste mancanze sarebbe stato possibile eseguire sul software dei codici capaci di modificare sia i report di Cellebrite relativi all'attacco sia quelli precedenti e futuri, creati a partire da dispositivi acquisiti in precedenza. Inoltre, sarebbe stato possibile attuare modifiche rilevanti nel contenuto analizzato: inserire o rimuovere parti testuali, messaggi di posta elettronica, immagini, contatti, file e qualunque tipo di dato, il tutto sfuggendo completamente ai controlli dei *checksum*. Nei casi peggiori, come riporta sempre Signal, un attacco simile avrebbe addirittura potuto causare la fuoriuscita dei dati presenti sul dispositivo analizzato, il tutto con ovvia ripercussione sull'attendibilità dell'analisi stessa[113].

Il caso appena esaminato rende evidente le maggiori criticità di *cyber security* che possono inficiare la funzionalità degli strumenti per le analisi forensi. Il rischio è che malware capaci di agire nei termini su visti possano presto divenire una realtà largamente diffusa.

Secondo gli esperti, tuttavia, si potrebbe ricorrere ad alcune contromisure. In particolare, per ovviare alle problematiche di file illeciti di questo genere una soluzione potrebbe essere quella di rivolgere lo sguardo agli strumenti di *machine learning*; ovvero a algoritmi che facendo ricorso a logiche matematiche e di elaborazioni computazionale sono in grado di apprendere informazioni direttamente dai dati che gli vengono sottoposti,

[111] L'articolo è consultabile sul sito Signal >> Blog >> Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective.

[112] Secondo quanto sostenuto da Signal, infatti, in realtà Cellebrite sarebbe riuscita semplicemente a capire dove si trovasse la chiave di cifratura con la quale i messaggi venivano localmente cifrati, cioè sul dispositivo analizzato, e non a forzare il meccanismo di cifratura delle chat dell'applicazione.

[113] Per un maggiore approfondimento si rimanda nuovamente a P. DAL CHECCO, op. cit., in Cybersecurity360.

senza che abbiano ricevuto in precedenza delle istruzioni specifiche. Una volta "addestrati" questi algoritmi sono in grado di adattarsi a situazioni nuove e potenzialmente, in chiave predittiva, a riconoscere programmi che si comportano in maniera difforme dalla normalità, potendo quindi teoricamente scoprire file malevoli che si camuffano da altri programmi.

L'applicazione delle logiche del *machine learning* alla *digital forensics*[114], in fase di esame della copia forense, potrebbe quindi aiutare il programma di analisi a individuare possibili programmi malevoli e catalogarli come file sospetti.

Su un piano più tecnico gli algoritmi di *machine learning*, operando una verifica dei metadati dei programmi presenti sulla copia, sarebbero in grado di comprendere se un file possa essere potenzialmente dannoso mediante un confronto con i metadati di programmi già noti al sistema o dal medesimo già considerati sospetti[115].

Di certo l'applicazione degli algoritmi di *machine learning* non può costituire l'unica soluzione. Una buona strategia difensiva non può prescindere, ad esempio, dal costante aggiornamento del sistema e dalla applicazione delle altre comuni buone pratiche e accorgimenti che costituiscono i principi fondanti della sicurezza informatica.

[114] Si rimanda a N. BASSETTI, "Machine learning per l'identificazione dei file sospetti: tecniche e sviluppi", in Cybersecurity360, consultabile sul sito https://www.cybersecurity360.it/soluzioni-aziendali/machine-learning-per-lidentificazione-dei-file-sospetti-tecniche-e-sviluppi/.

[115] *Ibidem*

FORUM ICT SECURITY 2023

Iscriviti alla newsletter di **ICT Security Magazine** per conoscere le prossime date, l'agenda e per partecipare alla **21ª Edizione del Forum ICT Security**

Sulla necessità di software di *digital forensics* direttamente gestiti e controllati dallo Stato

Casi come Cellebrite Ufed v. Signal pongono in luce come la *cyber security* sia un fattore essenziale per la corretta riuscita di un'indagine di *digital forensics*. In particolare, emerge come uno scarso livello di sicurezza del software utilizzato per l'analisi della copia forense rischi in concreto di tradursi in un'indagine fuorviante, dalla quale non potranno che conseguire risultati inattendibili. È opportuno, tuttavia, osservare come nell'assetto giuridico che disciplina la materia manchi del tutto una normativa tecnica che imponga livelli minimi di sicurezza nelle strumentazioni utilizzate. Sul punto, il rinvio del legislatore alle *best practices* – tra le quali ve ne sono di specifiche che si occupano di sicurezza – è l'unico appoggio normativo che possa rinvenirsi riguardo al dovere di rispettare criteri minimi di *cyber security*. Però, dal momento che la giurisprudenza ha stabilito come il mancato rispetto delle buone pratiche internazionali non comporti automaticamente l'inutilizzabilità delle evidenze digitali, sorge spontaneo chiedersi se la soluzione adottata sul piano legislativo si possa valutare sufficiente oppure se sia il caso di introdurre accorgimenti giuridici ulteriori. In realtà, se si prende in considerazione la rapidità con cui evolvono le minacce informatiche e se si considera l'entità del danno che un'indagine potrebbe subire in caso di mancanza d'uso di strumenti sicuri, appare palese come l'attuale impostazione della disciplina contenga un vuoto normativo che, in un contesto di crescente ricorso alle tecniche di *digital forensics*, corre il rischio di aumentare sempre più la percentuale di errori giudiziari.

La questione assume un tono di maggiore inquietudine se si considera che strumenti con acclarate vulnerabilità, come ad esempio la precedente versione del software Phisycal Anayzer di Cellebrite Ufed, sono stati largamente usati dalle procure e dalle forze

dell'ordine del nostro Paese e potenzialmente potrebbero tuttora essere in utilizzo presso i medesimi organi.

Il problema si pone dal momento che, non disponendo la Pubblica Amministrazione di strumenti e software di *digital forensics* prodotti direttamente dallo Stato, procure e forze dell'ordine per munirsi di simili sistemi sono costrette a rivolgersi ad aziende private, quasi sempre straniere. Tale circostanza, in assenza di una normativa specifica che disponga standard minimi di sicurezza, comporta che l'acquirente – in questo caso, gli organi statali – debbano necessariamente rifarsi ai livelli di sicurezza che propone l'azienda venditrice, la quale agendo secondo logiche privatistiche potrebbe talvolta ritenere non necessario incrementare le difese dei propri sistemi. Si rammenti, a titolo esemplificativo, che il precedente di Phisycal Analyzer veniva ad esistenza proprio a causa del mancato ammodernamento del software, che circolava con un aggiornamento obsoleto poiché non implementato da anni dalla casa produttrice.

Alla luce di quanto esposto, si presenta sempre più necessario il perfezionamento di un intervento normativo diretto a colmare il vuoto legislativo in tema di sicurezza e volto all'eliminazione delle attuali incertezze.

L'intervento, nello specifico, dovrebbe muoversi su due piani distinti ma connessi tra loro. Innanzitutto, andrebbero stabiliti dei livelli minimi di sicurezza che gli applicativi usati per le operazioni di *digital forensics* dovrebbero rispettare per poter essere adoperati ai fini d'indagine. In secondo luogo, occorrerebbe fare in modo che lo Stato sia messo concretamente nella posizione di valutare attivamente lo standard di sicurezza minima essenziale di tali applicativi.

Per fare ciò, bisognerebbe mettere a punto un sistema di controllo diretto dello Stato sulle aziende fornitrici: ipotesi allo stato attuale molto difficile, sia perché le maggiori aziende tech sono straniere e sia perché le medesime, in ottica di mercato, tendono a proteggere il segreto delle loro invenzioni, anche nei confronti degli Stati a cui offrono il servizio.

Oltre alla possibilità di creare dei software di completa proprietà dello Stato – in linea teorica la scelta migliore, ma in termini pratici di complessa realizzazione nonché estre-

mamente dispendiosa[116] – un'altra soluzione potrebbe essere incentivare la nascita di un gruppo di aziende conformi a specifici criteri, organizzate in consorzio e sottoposte alla diretta vigilanza dello Stato, che ne costituirebbe il primo fruitore dei servizi[117]. Una simile soluzione, se opportunamente regolata, permetterebbe allo Stato di imporre a tali aziende il rispetto di livelli di sicurezza minimi per i loro prodotti e la necessità di sottoporsi a controlli specifici che garantirebbero l'efficienza dei servizi e la più completa trasparenza al riguardo. Di ritorno, tali aziende avrebbero la certezza di un cliente sicuro quale la Pubblica Amministrazione.

È chiaro che una soluzione del genere andrebbe disciplinata a regola d'arte al fine di evitare situazioni di abuso e in ogni caso non sarebbe realizzabile nel breve termine.

Non vi è dubbio, tuttavia, che la questione della sicurezza informatica nella *digital forensics* debba essere quanto prima attenzionata a livello normativo; così da impedire da un lato che sia compromessa la genuinità delle indagini di informatica forense e dall'altro tutelando la posizione processuale dell'indagato

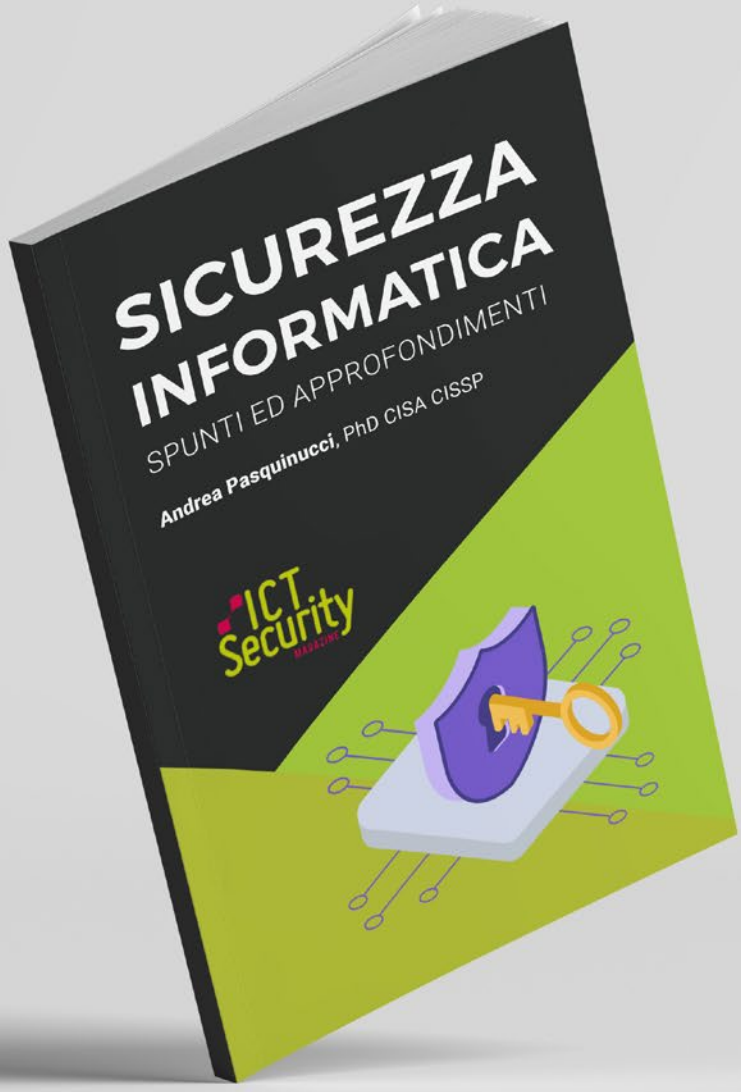
[116] Si consideri che il mondo della sicurezza è in continua evoluzione e, in ottica di spese, per lo Stato sviluppare software proprietari significherebbe investire in maniera continuativa somme di denaro molto ingenti obbligandolo ad uno sforzo economico di elevate proporzioni.

[117] Una soluzione simile è stata proposta anche per quanto riguarda la materia del captatore informatico, strumento che per molti aspetti, se non in maniera addirittura più rilevante, patisce dal punto di vista della *cyber security* delle medesime problematicità a cui soggiacciono gli strumenti informatici per la *digital forensics*. Si veda sul punto il servizio giornalistico intitolato *"Infiltrato speciale"*, curato da P. MONDANI nella trasmissione "Report", puntata del 18/11/2019.

Libro in versione **cartacea** ed **eBook**

SICUREZZA INFORMATICA

SPUNTI ED APPROFONDIMENTI



Il libro è distribuito gratuitamente a tutti gli iscritti alla newsletter di ICT Security Magazine

Conclusioni

La rivoluzione digitale che caratterizza l'attuale fase storica ha notevolmente impattato, tra gli altri, anche i settori del diritto processuale e delle scienze forensi. Qui, le nuove tecnologie stanno trovando larghissimo impiego soprattutto per quanto concerne l'ambito investigativo e il ricorso alle tecniche di *digital forensics* si rivela, sempre più di frequente, un elemento imprescindibile per gli inquirenti. L'analisi dei dispositivi elettronici rinvenuti sulla scena del crimine o in uso dall'indagato permette infatti di reperire informazioni, trovare indizi, collezionare elementi di prova e raggiungere risultati che le indagini tradizionali, in un mondo sempre più informatizzato, difficilmente riuscirebbero a ottenere.

Per contro, a causa della delicatezza che caratterizza questo tipo di operazioni, le potenzialità investigative della *digital forensics* si scontrano inevitabilmente con una serie di criticità.

Ove non adeguatamente tenuta in conto durante le fasi di acquisizione, analisi e catena di custodia, la fragilità della *digital evidence* rischia di compromettere da un lato il buon esito delle indagini e, dall'altro, le garanzie difensive del soggetto indagato, che nella normalità della casistica riveste, durante l'espletamento delle attività forensi, un ruolo meramente passivo.

Inoltre, proprio la natura digitale di questo tipo di indagine non lascia immune la digital forensics dai pericoli che riguardano il settore informatico in generale, imponendo la necessità di adottare opportuni accorgimenti anche per quanto concerne la sicurezza. Come dimostrato dai recenti casi di cronaca, infatti, il concetto di *cyber security* nella *digital forensics* non può assolutamente essere sottovalutato al fine di garantire la completa attendibilità dell'indagine.

Per quanto riguarda la disciplina normativa si è visto visto come in Italia, anziché regolare dettagliatamente la materia, sia stata scelta una strategia di rinvio alle c.d. *best practices* internazionali, inserendo all'interno del codice di procedura penale esclusi-

vamente l'obbligo, nel maneggiare le evidenze digitali, di fare ricorso a tecniche atte a preservare l'integrità e l'immodificabilità dei dati.

Questo atteggiamento legislativo, seppur giustificabile alla luce della continua evoluzione tecnologica, ha lasciato ampio spazio di manovra alla giurisprudenza; la quale, avendo chiarito la non obbligatorietà per gli inquirenti di rispettare le best practices, parrebbe aver addirittura ridimensionato il proposito della legge n. 48/2008.

Il nostro modello giuridico propone, attualmente, un contemperamento tra garanzie del diritto di difesa ed esigenze investigative nettamente sbilanciato in favore di queste ultime, ponendo l'indagato in una posizione oltremodo subalterna e relegandone le tutele costituzionali in secondo piano. Per tutelarne quanto più possibile la posizione processuale potrebbe essere utile, allora, trovare nuove strategie per anticipare il contraddittorio: ad esempio con la possibilità di nominare un consulente per la difesa che intervenga ancor prima della *discovery* delle prove. Si rammenta in proposito che la giurisprudenza ha ricompreso le operazioni di *digital forensics* tra gli atti ripetibili, eseguibili pertanto senza la necessità di integrare il contraddittorio con l'indagato: evenienza che tuttavia, unita alla possibilità di discostarsi dalle best practices, rischia di assumere i contorni propri del processo inquisitorio. Secondo l'attuale impostazione, infatti, l'onere probatorio (inquadrabile come *probatio diabolica*) di indicare come il discostamento dagli standard internazionali abbia compromesso le evidenze digitali ricade in capo all'indagato, anche laddove non abbia potuto partecipare alle operazioni.

La mancata previsione di una disciplina specifica in tema di *cyber security* può, inoltre, riverberarsi negativamente sull'attendibilità delle risultanze che vengano analizzate con strumenti di *digital forensics* non sostenuti da idonei sistemi di sicurezza. Andrebbero altresì previsti opportuni controlli sulle aziende fornitrici di questi servizi, per poter valutare l'efficienza dei prodotti in uso presso le Pubbliche Amministrazioni.

Alla luce di tali considerazioni appare ormai necessaria la creazione di un assetto normativo più dettagliato, che sappia calibrare correttamente il peso delle criticità che permeano una materia delicata come l'informatica forense per individuare il corretto bilanciamento tra esigenze investigative, *cyber security* e diritto di difesa.

Bibliografia e sitografia[118]

- S. ATERNO, *"Digital forensics e scena criminis"*, in *"Manuale delle investigazioni sulla scena del crimine Norme, tecniche, scienze, logica"* a cura di D. CURTOTTI e L. SARAVO, G. Giappichelli Editore, Pioltello (MI), 2019
- N. BASSETTI, *"Machine learning per l'identificazione dei file sospetti: tecniche e sviluppi"*, in Cybersecurity360, sul sito https://www.cybersecurity360.it/soluzioni-aziendali/machine-learning-per-lidentificazione-dei-file-sospetti-tecniche-e-sviluppi/
- L. BARTOLI e C. MAIOLI, *"La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti"*, in Informatica e diritto, XLI annata, Vol. XXIV, 2015, n. 1-2
- G. BRAGHÒ, *"L'ispezione e la perquisizione di dati, informazioni e programmi informatici"*, in Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008, n. 48)" a cura di L. LUPARIA, Milano, 2009
- F. CAJANI, *"Il vaglio dibattimentale della digital evidence"*, in Archivio Penale, settembre-dicembre 2013, fasc. 3, anno LXV
- F. CAJANI, *"La cooperazione internazionale nelle indagini digitali"*, in "Cyber forensics e indagini digitali Manuale tecnico-giuridico e casi pratici", a cura di S. ATERNO, F. CAJANI, G. COSTABILE e D. CURTOTTI, G. Giappichelli Editore, Pioltello (MI), 2021
- V. CALABRÒ, G. COSTABILE, S. FRATEPIETRO, M. IANULARDO, G. NICOSIA, *"L'alibi informatico: aspetti tecnici e giuridici"*, sul sito https://www.vincenzocalabro.it/pdf/2010/AlibiInformatico.pdf
- V. G. CALABRÒ, *"La fragilità della prova informatica: caratteristiche generali e problematiche emergenti"*, consultabile sul sito: https://www.vincenzocalabro.it/pdf/2008/LaProvaInformatica.pdf

- O. CALAVITA, *"L'odissea del trojan horse, Tra potenzialità tecniche e lacune normative"*, in Diritto Penale Contemporaneo, fasc. 11/2018
- E. CASEY, *"Digital Evidence and Computer Crime"*, III ed., Waltham, Academic Press, 2011
- E. CASEY, *"Error, Uncerainty and Loss in Digital Evidence"*, in International Journal of Digital Evidence, Vol. 1, 2002, sul sito www.utica.edu
- A. COLAIOCCO, *"La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria"*, in Archivio Penale – Cultura penale e spirito europeo, n. 1 del 2019
- F. COLAIUDA, *"La qualità dell'investigazione sulla scena del crimine – il metodo di lavoro basato sui protocolli operativi e sulle check lists"*, p. 1, sul sito http://www.associazionelaic.it/wp-content/uploads/2018/07/Colaiuda-3.pdf
- R. COLUCCINI, *"Errori giudiziari: come la prova tecnologica manda in carcere un innocente"*, in Irpimedia, sul sito https://irpimedia.irpi.eu/prova-tecnologica-caso-mered/
- A. CONTALDO e F. PELUSO, *"E-detective: l'informatica giuridica e le applicazioni della Digital Forensics"*, PM Edizioni, Verazze (SV), 2018
- G. COSTABILE, *"Digital forensics & digital investigation: classificazione, tecniche e linee guida nazionali ed internazionali"*, in *"Cyber forensics e indagini digitali Manuale tecnico-giuridico e casi pratici"*, a cura di S. Aterno, F. CAJANI, G. COSTABILE e D. CURTOTTI, G. Giappichelli Editore, Pioltello (MI), 2021
- D. CURTOTTI, *"Attività di acquisizione della digital evidence: ispezioni, perquisizioni e accertamenti tecnici"*, in *"Cyber forensics e indagini digitali Manuale tecnico-giuridico e casi pratici"*, a cura di S. ATERNO, F. CAJANI, G. COSTABILE e D. CURTOTTI, G. Giappichelli Editore, Pioltello (MI), 2021
- D. CURTOTTI, *"Il sequestro"*, in *"Cyber forensics e indagini digitali Manuale tecnico-giuridico e casi pratici"*, a cura di S. ATERNO, F. CAJANI, G. COSTABILE e D. CURTOTTI, G. Giappichelli Editore, Pioltello (MI), 2021

- D. CURTOTTI, *"Rilievi e accertamenti sul locus commissi delicti nelle evoluzioni del codice di procedura penale"*, in *"Manuale delle investigazioni sulla scena del crimine Norme, tecniche, scienze, logica"*, a cura di D. CURTOTTI e L. SARAVO, G. Giappichelli Editore, Pioltello (MI), 2019
- P. DAL CHECCO, *"Hacking-Boat 2019 – Digital Forensics"*, sul sito https://hackinboat.it/wp-content/uploads/2019/05/HackInBoat-Digital-Forensics-Paolo-Dal-Checco.pdf
- P. DAL CHECCO, *"Signal ha hackerato Cellebrite, svelate vulnerabilità nelle app di hacking telefonico: i risvolti"*, in Cybersecurity360, sul sito https://www.cybersecurity360.it/nuove-minacce/signal-ha-hackerato-cellebrite-svelate-vulnerabilita-nelle-app-di-hacking-telefonico-i-risvolti/
- M. DANIELE, *"La prova digitale nel processo penale, in Riv. dir. proc., 2011, p. 283, Cfr. M. PITTIRUTTI, Digital evidence e procedimento penale"*, G. Giappichelli editore, 2017
- R. DE VITA e L. LAUDISA, *"Vita digitale a rischio: i captatori informatici tra pericoli per i diritti umani e riduzionismo giuridico"*, in Osservatorio CyberSecurity Eurispes, articolo del 18 novembre 2019, sul sito https://www.devita.law/wp-content/uploads/2019/11/Vita-digitale-a-rischio.pdf
- V. FROSINI, *"Implicazioni sociali dei vantaggi e degli svantaggi della rivoluzione informatica"*, in "Informatica e diritto", Vol. XIII, Fasc. 3, 1987
- T. E. FROSINI, *"Il diritto costituzionale di accesso ad Internet"*, in "AIC Associazione Italiana dei Costituzionalisti", n. 1 del 2011, data di pubblicazione 15/12/2010
- N. FUSARO, *"Delitti e condanne… Prova scientifica e ragionevole dubbio"*, in Osservatorio del Processo Penale, 2009
- N. FUSARO, *"La sentenza assolutoria della Corte di assise d'appello di Perugia per l'omicidio di Meredith Kercher, tra valutazione della prova scientifica e prevalenza del principio dell'oltre ogni ragionevole dubbio. L'analisi del criminologo"*, in *"L'assassino di Meredith Kercher"*, Aracne, 2012
- A. GAMMAROTA con relatore C. MAIOLI, *"Informatica forense e processo penale: la*

prova digitale tra innovazione normativa e incertezze giurisprudenziali" [dissertation thesis], 2016, sul sito http://amsdottorato.unibo.it/7723/1/Gammarota_Antonio_tesi.pdf

- R. GENNARI e L. SARAVO, *"Tecnica, tecnologia e scienza sulle tracce del reato – Le tracce"*, in *"Manuale delle investigazioni sulla scena del crimine Norme, tecniche, scienze, logica"*, a cura di D. Curtotti e L. Saravo, G. Giappichelli Editore, Pioltello (MI), 2019
- F. GIUNCHEDI, *"Le malpractices nella digital forensics Quali conseguenze sull'inutilizzabilità del dato informatico?"*, in Archivio Penale, settembre–dicembre 2013, fasc. 3, anno LXV
- G. C. KESSLER, *"Anti-Forensics and the Digital Investigator"*, 2007, sul sito https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.258.5244&rep=rep1&type=pdf
- V. R. KOSTORIS, *"Ricerca e formazione della prova elettronica: qualche considerazione introduttiva"*, in F. RUGGERI e L. PICOTTI, *"Nuove tendenze della giustizia penale di fronte alla criminalità informatica: aspetti sostanziali e processuali"*, Giappichelli, Torino, 2011
- M. LIMONE, *"Cloud computing – aspetti contrattuali, risvolti normativi e tutela della privacy"*, Tricase (LE), 2018
- E. LORENZETTO, *"Le attività urgenti di investigazione informatica e telematica", in Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008, n. 48)"* a cura di L. LUPARIA, Milano, 2009
- F. MASSA, *"Il caso San Bernardino: APPLE vs FBI"* in sicurezzaegiustizia.com, consultabile sul sito https://www.sicurezzaegiustizia.com/il-caso-san-bernardino-apple-vs-fbi/
- L. MARAFIOTI, *"Digital evidence e processo penale"*, in Cass. Pen., 2011
- P. MONDANI, *"Infiltrato speciale"*, trasmissione Report, puntata del 18/11/2019
- R. MURENEC, *"Digital Forensics Aspetti tecnico-giuridici e operativi su trattamento dei dati digitali"*, Egaf Edizioni Srl, 2021

- F. PELUSO e M. FERNANDES DOS SANTOS, *""Battlefield digital forensics": la raccolta della prova informatica negli scenari di guerra"*, in IISFA Memberbook 2019-2020 DIGITAL FORENSICS, a cura di G. COSTABILE, A ATTANASIO e M. IANULARDO
- G. PIERRO, *"Introduzione allo studio dei mezzi di ricerca della prova informatica"*, in Dir. Pen. proc., 2011
- M. PITTIRUTI, *"Dalla Corte di Cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus"*, in Sistema Penale, sul sito https://www.sistemapenale.it/it/scheda/cass-sez-vi-sent-22-settembre-2020-dep-2-dicembre-2020-n-34265-pres-di-stefano-rel-silvestri
- M. PITTIRUTI, *"Digital evidence e procedimento penale"*, G. Giappichelli editore, 2017
- R. RIJITANO, *"Brute force: cosa sono, come fare e prevenire gli attacchi a forza bruta"*, in Cybersecurity360, sul sito https://www.cybersecurity360.it/nuove-minacce/brute-force-cosa-sono-gli-attacchi-a-forza-bruta-come-farli-e-prevenirli/
- M. TORRE, *"Sull'obbligo per il privato di collaborare ad attività di digital forensics – "Il caso Apple F.B.I."", In "Trattato di diritto penale – Cybercrime"*, a cura di A. CADOPPI, S. CANESTRARI, A. MANNA e M. PAPA, UTET Giuridica, Vicenza, 2019
- A. VITALE, *"La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico",* in Dir. Internet, 2008
- M. VITIELLO, *"Il laboratorio di informatica forense: i software, gli strumenti hardware, i costi"* sul sito https://www.agendadigitale.eu/documenti/il-laboratorio-di-informatica-forense-i-software-gli-strumenti-hardware-i-costi
- G. ZICCARDI, *"L'ingresso della computer forensics nel sistema processuale italiano"*, in *"Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008, n. 48)"* a cura di L. LUPARIA, Milano, 2009

- https://www.treccani.it/enciclopedia/rivoluzione-digitale_%28altro%29/
- https://www.treccani.it/enciclopedia/prova-scientifica_%28Lessico-del-XXI-Secolo%29/
- https://www.treccani.it/vocabolario/hardware/
- https://www.treccani.it/enciclopedia/crittografia/#:~:text=crittografia%20Tecnica%20di%20rappresentazione%20di,a%20trasformazioni%20che%20lo%20rendano
- https://www.bit4law.com/blog/informatica-forense-incident-response/gabbia-di-faraday-informatica-forense/
- https://www.dmi.unict.it/~battiato/CF1213/Lezione02%20-%20ISO%20e%20misurazione%20alterazioni.pdf
- Signal >> Blog >> Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective

[118] Sitografia consultata l'ultima volta nel mese di marzo 2022

Giurisprudenza citata

- Cass. Pen., Sez. I, n. 301 del 14 marzo 1990
- Cass. Pen., Sez. IV, n. 637 del 14 aprile 2004
- Tribunale di Bologna, Sent. n. 1823 del 22 dicembre 2005
- Cass. Pen., Sez. I, n. 239101 del 16 gennaio 2008
- Corte di Appello di Bologna, Sent. n. 369 del 27 marzo 2008
- Cass. Pen., Sez. I, n. 14511 del 5 marzo 2009
- Cass. Pen., II Sez., n. 11135 del 13 marzo 2009
- Cass. Pen., Sez. I, n. 23035 del 30 aprile 2009
- Tribunale di Vigevano, Sent. del 17 dicembre 2009
- Cass. Pen., Sez. III del 19 gennaio 2010
- Cass. Pen., Sez. V, n. 11905 del 16 novembre 2011
- Cass. Pen., Sez. V, n. 8736 del 16 gennaio 2018
- Corte d'Assise Tribunale di Palermo, Sent. del 12 luglio 2019
- Cass. Pen., Sez. IV, n. 34256 del 9 settembre 2020
- Cass. Pen., Sez. VII, n. 11066 del 10 febbraio 2021
- Cass. Pen., Sez. VI, n. 18907 del 20 aprile 2021

CYBER CRIME CONFERENCE 2023

Iscriviti alla newsletter di **ICT Security Magazine** per conoscere le prossime date, l'agenda e per partecipare alla **11ª Edizione della Cyber Crime Conference**

ICT Security MAGAZINE

ISCRIVITI ALLA NEWSLETTER

per ricevere aggiornamenti sulle prossime iniziative. Seguici sui canali social: Linkedin, Facebook, Twitter