https://doi.org/10.6092/issn.1825-1927/21507 ISSN 1825-1927

Il percorso della prova digitale nelle attività di Digital Forensics, una review

Giuseppe Verde [1]

[1] Università degli Studi di Napoli Federico II, Italia

Abstract: L'informatica forense è la disciplina che si occupa dell'identificazione, acquisizione, analisi e conservazione di prove digitali, contribuendo all'accertamento di fatti in ambito giuridico. Originariamente nata come supporto alle indagini penali, si è progressivamente estesa anche ai procedimenti civili, amministrativi e tributari, a seguito della crescente digitalizzazione della società. La delicatezza della prova informatica, caratterizzata da volatilità e rischio di alterazione, impone metodologie rigorose per garantirne integrità, autenticità e ammissibilità nel processo. L'ordinamento italiano ha introdotto la disciplina dell'informatica forense con la legge n. 547/1993, per poi adeguarsi agli standard internazionali con la ratifica della Convenzione di Budapest del 2001 (legge n. 48/2008), che ha delineato le linee guida per la gestione delle prove digitali e la catena di custodia. Nonostante l'assenza di normative operative univoche in Italia, la comunità scientifica adotta protocolli ispirati a standard internazionali come la RFC3227. Un ruolo centrale nelle indagini è ricoperto dai dispositivi mobili, in particolare gli smartphone, che costituiscono veri e propri archivi digitali di dati personali e comunicazioni. L'analisi forense di tali dispositivi presenta sfide legate alla varietà di hardware, software e sistemi operativi, nonché alla sicurezza e alla cifratura dei dati. L'evoluzione dell'intelligenza artificiale e della data science sta fornendo nuove opportunità di analisi e investigazione, ma le minacce informatiche sempre più sofisticate complicano il lavoro degli esperti forensi. Nel contesto attuale delle indagini digitali, emergono criticità che riguardano non solo gli aspetti tecnici, ma anche la trasparenza e l'accessibilità delle operazioni, soprattutto nelle fasi di acquisizione e conservazione della prova. Il coinvolgimento marginale dello specialista forense solleva dubbi sull'equilibrio tra esigenze investigative e garanzie epistemologiche.

Keywords: Digital Forensics, Mobile Forensics, Chain of Custody, Digital Evidence.

1 Introduzione

A partire dalla prima definizione di cui si ha traccia nella letteratura italiana[1] che qualificava l'Informatica forense (IF) come «la disciplina che studia l'insieme delle attività che sono rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova»[2], i

giuseppe.verde@unina.it (Giuseppe Verde);
(Giuseppe Verde);

1. La definizione che si attribuisce a Cesare Maioli è precedente al 2004. C. Maioli, *Dar voce alle prove: elementi di informatica forense,* in P. Pozzi (a cura di) *Crimine virtuale, minaccia reale*, F. Angeli, 2004.

2. Per una introduzione di ruolo, principi e metodi della informatica forense si veda G. Ziccardi, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in L. Lupária (a cura di), *Sistema penale e criminalità informatica,* Giuffrè, Milano, 2009; P. Perri, voce *Computer forensics (indagini informatiche)*, in Digesto delle discipline penalistiche, Utet, Torino, 2011; G. Fagioli, A. Ghirardini, *Digital forensics,* Apogeo, 2020 e S. Aterno, F. Cajani, G. Costabile, D. Curtotti (a cura di), *Cyber Forensics e indagini digitali*, Giappichelli, 2021. Inoltre, E. Casey *Foundations of digital*

confini della materia si sono prepotentemente dilatati, spinti dalla sempre crescente dipendenza della società moderna dalle tecnologie informatiche.

L'Informatica forense, in quanto area dell'informatica giuridica, si occupa della identificazione, acquisizione e analisi giudiziale del contenuto informativo di dispositivi e sistemi informatici. È dunque una scienza forense che, al pari di altre scienze (quali la medicina legale e la balistica forense), si è dapprima proposta come scienza ausiliaria nel processo penale, per poi entrare oggi nella quasi totalità dei procedimenti giudiziari[3].

Infatti, l'Informatica forense appare naturalmente inquadrabile tra le scienze ausiliare all'applicazione del diritto penale e processuale penale, secondo la tradizione classificatoria dei più importanti Autori di tali discipline[4].

La trasversalità delle problematiche studiate dall'Informatica forense rispetto a molti altri ambiti diversi dal diritto penale e processuale penale, è resa attuale dalla pervasività dei cambiamenti tecnologici e sociali e dalle recenti riforme legislative verificatesi in vari settori del diritto processuale che hanno toccato gli ambiti del processo tributario, amministrativo e civile[5].

La prova informatica può essere definita come "la rappresentazione di un insieme di dati ed informazioni digitalizzate, facenti capo ad un determinato fatto o evento, informazioni che sono espresse in linguaggio informatico, un linguaggio che, per sua stessa natura, non è immediatamente intellegibile dall'uomo attraverso i suoi sensi"[6]. I sistemi informatici utilizzano un linguaggio binario, fatto di 0 e di 1, per memorizzare le informazioni. Tale linguaggio non è comprensibile dall'uomo che necessita di software utilizzati all'interno di sistemi operativi memorizzati su Hard Disk o altri supporti digitali per comprenderne il contenuto. L'obiettivo principale dell'indagine è quello dell'acquisizione e l'individuazione dell'autore del fatto che, spesso, può avere agito in un luogo assai distante da quello dove il reato si è manifestato.

Sia l'acquisizione della prova del fatto che l'individuazione di chi ha agito potrebbero risultare estremamente difficili poiché le tracce informatiche possono essere nascoste o distrutte e chi ha operato può cercare di rendersi il meno possibile individuabile[7].

Gli esperti informatici forensi si trovano a dover cercare traccia di accadimenti in "luoghi" che fino a poco tempo fa era impensabile potessero contenere dati rilevanti per l'accertamento di un fatto: telecamere di sorveglianza, stampanti 3D, apparecchiature biomedicali e autoveicoli[8]. Il ricorso a informazioni desunte dai dati digitali conservati in supporti informatici o trasmessi attraverso le reti non riguarda solo il procedimento penale ma si estende a qualsiasi contesto in cui diventi necessario produrre, a sostengo della propria tesi, quelle che sono "rappresentazioni informatiche" di fatti (ad esempio e-mail, messaggi, post su piattaforme web)[9].

---

forensics, in ID. (ed.) *Digital evidence and computer crime*, 3rd ed. Academic, Waltham, 2011; L. Daniel, *Digital forensics for legal professionals. Understanding digital evidence from the warrant to the courtroom*, Syngress, Amsterdam, 2012; J. Henseler, *Computer crime and computer forensics*, in The Encyclopaedia of Forensic Science, Academic, London, 2000; S. Mason, *Electronic evidence*, 3rd ed., Lexis Nexis Butterworths, London, 2012. Si v. anche M. Pollit, *A History of Digital Forensics*, in K.P. Chow-S. Shenoi (eds.), *Advances in Digital Forensics* VI, Boston, Springer, 2010, pp. 3-15.

3. R. Brighi, *Informatica forense, algoritmi e garanzie processuali*, 2001. Pollit (2010) ricostruisce la storia della disciplina. Per l'inquadramento dei principi e metodi dell'Informatica forense in Italia si vedano, tra tutti, Maioli (2004,2015).

4. *Ex multis:* F. Antolisei, *Manuale di diritto penale, Parte generale*, Giuffrè, 1987, p. 26.; F. Mantovani, *Diritto Penale, Parte generale*, Cedam, 1992, p. 10.

5. C. Maioli, *Nuove questioni di informatica forense*, R. Brighi (a cura di), Aracne, Roma, 2022.

6. L. Luparia, G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007.

7. G. Bragò, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in L. Luparia, Sistema e criminalità informatica, Giuffrè, Milano, 2009.

8. M. Ferrazzano, *Dai veicoli a guida umana alle autonomous car. Aspetti tecnici e giuridici, questioni etiche e prospettive per l'informatica forense*, Giappichelli, 2018.

9. Nel processo civile, in ambito giuslavorista, in materia di diritto amministrativo, ma anche nelle investigazioni aziendali (Corporate Digital forensics), allo scopo di individuare eventuali attacchi informatici provenienti dall'esterno, scoprire dipendenti infedeli, attività di spionaggio, furto o danneggiamento dei dati, violazione delle policy aziendali e in ambito sanitario per la gestione del rischio clinico (informatica forense sanitaria). Gli esempi sono molteplici. Tra tutti si vedano: A. Gammarota, D. Caccavella, *L'informatica forense per l'E-Health*, in C. Faralli, R. Brighi, M. Martoni (a cura di) *Strumenti, diritti, regole e nuove relazioni di cura. Il paziente europeo protagonista nell'eHealth*, Giappichelli, 2015, pp. 205-220; U. Bardari, *L'esperimento giudiziale*

Gli strumenti standard utilizzati nelle procedure di IF coprono tutti i diversi aspetti delle fasi di indagine informatica e seguono il dato nel suo ciclo di vita completo: dall'individuazione e acquisizione delle potenziali prove digitali, alla loro analisi, valutazione e conservazione, fino alla chiusura dell'indagine[10]. Ogni operazione manuale o automatizzata è condotta salvaguardando i requisiti tecnici di verificabilità, ripetibilità, riproducibilità e giustificabilità secondo il paradigma dalla catena di custodia[11].

In primissima approssimazione, essa consente di individuare le fasi del trattamento del dato digitale, potendo verificare ex post i diversi passaggi attraverso la documentazione: quest'ultima si può considerare come il vero tracciamento delle procedure che conducono al repertamento e all'analisi dei dati digitali[12]. In tale fase vanno poi osservate specifiche misure tecniche[13] finalizzate a tutelare l'integrità dell'elemento raccolto[14].

La fragilità del dato informatico, per le sue congenite caratteristiche effimere, impone di considerare con particolare attenzione le fasi dell'acquisizione e della conservazione della prova digitale, maggiormente suscettibili di comprometterne l'integrità e l'autenticità del dato informatico acquisito[15]. In questo contesto la polizia giudiziaria ha l'esigenza di valutare il ruolo e la natura delle "impronte elettroniche", di individuare quali supporti informatici possono contenere potenziali tracce del reato, di acquisire e preservare le fonti di prova fino alla loro successiva analisi laddove non fosse possibile espletare i dovuti accertamenti direttamente sul posto[16]. L'informatica ci insegna che i dati digitali, per loro caratteristica, possono essere copiati 'bit to bit', cosicché si può ottenere una copia identica dell'originale (c.d. copia-clone o bitstream): tant'è che dal punto di vista informatico la copia originale e la copia-clone non sono differenziabili[17].

È evidente che la copiatura forense sia una prova scientifica, la cui caratteristica essenziale risiede nel momento acquisitivo caratterizzato dall'ausilio di conoscenze e metodologie attinenti a sapere scientifico e tecnico[18].

In questo contesto, si evidenziano ulteriori criticità non soltanto sul piano tecnico, ma anche in relazione all'accessibilità e alla trasparenza delle attività di indagine, specie nelle fasi più delicate di acquisizione e conservazione della prova digitale. La possibilità per lo specialista forense di contribuire in modo tempestivo e consapevole all'analisi delle evidenze risulta, in molte circostanze, subordinata a prassi operative e a scelte investigative che tendono a rimanere poco permeabili all'apporto tecnico indipendente. Tale condizione solleva interrogativi significativi in merito all'equilibrio tra esigenze investigative e garanzie epistemologiche nella costruzione del fatto processuale e merita, anche alla luce delle trasformazioni normative in atto, un'attenta riflessione.

---

su posizionamento GPS e scatole nere per automobili, in R. Brighi, M. Palmirani, E. Sánchez Jordán (a cura di), *Informatica giuridica e informatica forense al servizio della società della conoscenza*, Aracne, 2018, pp. 241-254.

10. I passaggi di cui si compone la Digital investigation sono descritti in particolare, nella norma tecnica ISO/IEC 27043 «Information technology – Security techniques – Incident investigation principle and processes».

11. Requisiti fissati dalle norme tecniche di riferimento e in particolare dalla ISO/IEC 27037. Sulla catena di custodia L. Bartoli, C. Maioli, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in M. A. Biasiotti, M. Epifani, F. Turchi (a cura di), *Trattamento e scambio della prova digitale in Europa*, Edizioni Scientifiche Italiane, 2016, pp. 139-151.

12. P. Perri, voce, *Computer forensics (indagini informatiche)*, in *AA.VV*., Dig. pen., Utet, IV Agg., 2011, p. 100.

13. Ne ripercorre alcune, sottolineando l'importanza di lavorare sulla copia dei dati e non sull'originale, S. Raghavan, *Digital Forensic Research: Current State of Art,* in *CSI transactions on ICT*, 2013, n. 1, p. 91.

14. *Rule of Evidence n. 901*, che recita *«To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is».*

15. Per una disamina esaustiva della necessità di acquisire correttamente il dato informatico, si veda C. Maioli, *Dar voce alle prove: elementi di informatica forense*, in P. Pozzi, R. Masotti e M. Bozzetti (a cura di), *Crimine virtuale, minaccia reale*, a cura di Franco Angeli, 2004. Sull'importanza della corretta metodologia da adottare nel trattamento della prova informatica, dalla sua acquisizione alla successiva analisi, si veda S. Aterno, P. Mazzotta, *La perizia e la consulenza tecnica – con approfondimento in tema di Perizie Informatiche* (analisi e schede tecniche di D. Caccavella), CEDAM, 2006.

16. L. Cuomo, *La prova digitale*, in G. Canzio - L. Luparia (a cura di) *Prova scientifica e processo penale*, CEDAM, 2017.

17. S. Golin, *Questioni aperte sull'acquisizione probatoria di dati informatici (*a cura di) R. Brighi, *Nuove questioni di informatica forense*, Aracne, Roma, 2022.

18. O. Dominioni, *La prova penale scientifica*, Giuffrè, 2005.

2 L'Informatica forense entra a far parte dell'ordinamento penale italiano

L'intervento del Legislatore italiano nato a contrastare in sede penale la cosiddetta criminalità informatica risale al 1993, con la legge n. 547. L'introduzione di tale disciplina si rese necessaria poiché il tentativo di applicare ai comportamenti criminosi commessi attraverso l'uso del personal computer e della rete informatica o anche alle condotte realizzate ai danni dei sistemi informatici altrui le fattispecie delittuose presenti nel codice penale, appariva un'operazione di dubbia fattibilità e comunque passibile di violazione dei principi di tassatività e legalità del diritto penale; l'inadeguatezza degli strumenti posti a disposizione del penalista rendeva pressoché privi di sanzione i comportamenti di cybercrime e proprio a tale carenza volle rispondere l'intervento normativo del 1993[19].

In ambito internazionale, a meno di 10 anni da questa riforma, è emerso un nuovo e più intenso bisogno di repressione delle condotte criminose realizzate attraverso l'utilizzo di attrezzature informatiche. Approvando il consiglio d'Europa la Convenzione di Budapest[20] in data 23 Novembre 2001, la valenza e la rilevanza internazionale del fenomeno del cybercrime hanno trovato pieno riconoscimento. Tale Convenzione rappresenta il primo accordo internazionale riguardante i reati commessi tramite Internet o altre reti informatiche.

Tale Convenzione da parte del Parlamento italiano è stata ratificata abbastanza recentemente con la legge 18 marzo 2008 n. 48, la quale ha introdotto innovazioni di assoluto rilievo, con una riscrittura della previgente disciplina di carattere sostanziale ed alcune significative modifiche anche in tema di diritto penale processuale[21]; dettando regole cautelari nell'acquisizione della prova digitale, indicando le esigenze che debbono essere soddisfatte, ma lasciando l'operatore libero nell'individuazione degli strumenti tecnici da utilizzare[22].

Grazie a questa innovazione legislativa si è introdotto nell'ordinamento penale italiano l'Informatica forense: le novità apportate con la legge n. 48 del 2008[23], infatti, racchiudono le linee guida che regolamentano la trattazione dei dati e la validazione al fine di poterli impiegare in un procedimento giudiziario[24]; tra queste assume una grande importanza la conservazione dei dati attraverso l'utilizzo di metodologie che escludano in modo certo il verificarsi di un'alterazione degli stessi: è il cosiddetto concetto di "catena di conservazione" del dato digitale.

Il concetto di "conservazione di un reperto informatico e di disponibilità del dato" sono i punti fondamentali di tutta la dottrina informatico forense. Il dato in formato digitale è, per sua natura, volatile e qualsiasi intervento esterno, anche involontario, può causarne una modifica.

---

19. F. Mucciarelli, Commento alla legge 23 dicembre 1993 n.547. *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, in Leg. Pen., Utet, Torino, 1996.

20. La Convenzione di Budapest del 23.11.2001 del Consiglio d'Europa sulla criminalità informatica è il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche. Importante notare che tra i firmatari troviamo sia stati membri UE che stati non membri UE; sul tema, tra gli altri: L. Picotti, *Ratifica alla Convenzione cybercrime e nuovi strumenti di contrasto alla criminalità informatica e non solo*, in Diritto dell'internet n. 5, 2008; C. Maioli e E. Sanguedolce, *I nuovi mezzi di ricerca della prova fra informatica forense e L. 48/2008*, Altalex, 7/5/2012.

21. L. Picotti, *Ratifica alla Convenzione cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo,* in Diritto dell'internet, Ipsoa, Milano, 2008.

22. Principio ribadito da Cass. Sez. 3 n. 3744 del 28/05/2015 Rv. 265180: «in tema di perquisizione di sistema informatico o telematico, sia l'art. 247, comma 1-bis, che l'art. 260, comma secondo, cod. proc. pen., si limitano a richiedere l'adozione di misure tecniche e di procedure idonee a garantire la conservazione dei dati informatici originali e la conformità ed immodificabilità delle copie estratte per evitare il rischio di alterazioni, senza imporre misure e procedure tipizzate. (Fattispecie in cui la Corte ha rigettato il motivo di ricorso genericamente fondato sulla mancata indicazione, da parte del consulente tecnico del PM, del cd. valore "hash" dei files ottenuti dai supporti informatici, in assenza peraltro di contestazione circa la mancata corrispondenza fra le copie estratte e i dati originariamente presenti sui supporti informatici nella disponibilità dell'imputato)».

23. Giova precisare che, se a livello internazionale e sovranazionale vi sono delle linee guida relative alla corretta analisi dei dispositivi mobili, in Italia l'unico punto di riferimento normativo è la l. 48/2008; pertanto, è necessario basarsi sui criteri sovranazionali elaborati dall'ISO (International Organization for Standardization) e dall' IEC (International Electro technical Commission) n. 27037/2012 e 27042/2015, che stabiliscono i criteri per ricavare la *digital evidence*, non disponendo di un adeguato supporto normativo interno in termini di corretta acquisizione e analisi della stessa.

24. F. Corona, *Le attività di digital forensics nel cybercrime, in Reati informatici e investigazioni digitali,* Pacini Giuridica, 2021.

La stessa procedura di acquisizione, se non eseguita con estrema perizia, può causare una modifica al dato originale o determinare che la copia non rispecchi fedelmente l'originale. Entrambe le situazioni determinano la futura impossibilità di poter impiegare l'informazione a fini probatori[25]. Per garantire una corretta catena di conservazione è importante operare in modo corretto fin dalle fasi di accesso alla scena del crimine in cui si procede alla ricerca e individuazione della strumentazione impiegate durante la commissione del reato, sia esso un reato strettamente informatico oppure un reato commesso attraverso l'uso di strumenti informatici od ancora nei casi in cui il sistema informatico semplicemente contiene informazioni utili o collaterali a comprendere e descrivere la scena del crimine[26].

In particolare, le procedure tipiche di IF secondo un autorevole studio[27] possono essere ricondotte a tre principali ambiti: (1) analisi di dati archiviati e *file system*, (2) analisi del traffico di rete e (3) *reverse engineering*, ciascuno dei quali si scontra con ostacoli e limiti dovuti all'evoluzione delle ICT[28].

In Italia non esistono normative ufficiali o delle linee guida pubblicate da enti governativi che definiscano in modo univoco le modalità operative per l'acquisizione e la trattazione dei dati digitali nel corso di un'indagine informatica: con l'introduzione delle modifiche del codice di procedura penale nel corso del 2008 sono stati definiti solamente alcuni requisiti minimi, idonei a salvaguardare l'originalità dei dati attraverso l'uso di strumentazioni appropriate[29].

In realtà le previsioni della legge del 2008 rispecchiano perfettamente quanto descritto nella RFC3227[30], che peraltro costituisce per la comunità scientifica e per il mondo giuridico il riferimento per la certificazione dell'iter operativo da adottare nello svolgimento delle attività di acquisizione di informazioni digitali[31].

Un sistema può essere ammissibile quando sia stato acquisito tramite strumenti che rispettino gli obblighi legislativi vigenti e supportato da idonea documentazione, mentre

risulta autentico e completo se è possibile comprovare l'integrità attraverso, ad esempio, la verifica dei contenuti attraverso una *funzione di hash*; l'autenticità e la completezza dovranno essere comprovate anche dalla documentazione della catena di conservazione. In pratica l'evidenza informatica potrà essere considerata attendibile solamente se non sussistono dubbi su come sia stata acquisita e successivamente manipolata, evitando che si possano sollevare dubbi in merito alla veridicità[32].

Le nuove competenze nell'intelligenza artificiale e nella data science si stanno, inoltre, unendo al campo della *Digital forensics* a supporto dell'analisi delle attività criminali e, più in generale, delle attività di intelligence[33].

La raccolta di informazioni provenienti da fonti diverse, tra cui sorgenti aperte, e la conseguente esplorazione con metodi e tecniche che mirano a identificare regolarità e relazioni all'interno di grandi dataset dove la capacità analitica umana sarebbe insufficiente[34], fornisce un aiuto alla comprensione generale dei fenomeni e

25. A. Ghirardini, G. Faggioli, *Computer Forensics*, Apogeo, Milano.

26. F. Cajani, S. Aterno, *Aspetti giuridici comuni delle indagini informatiche*, in S. Aterno, F. Cajani, G. Costaile, M. Attiucci, G. Mazzaraco, *Computer forensics e indagini digitali*, Experta, Milano, 2011.

27. L. Caviglione, S. Wendzel, W. Mazurczyk, *The Future of Digital Forensics: Challenges and the Road Ahead*, in IEEE Security & Privacy, 2017, 15(6), pp. 12-17.

28. *Information and Communication Technology*, ovvero l'insieme delle tecnologie utilizzate per acquisire, elaborare, trasmettere e conservare informazioni in formato digitale.

29. O. Signorile, Computer Forensic Guidelines: *un approccio metodico-procedurale per l'acquisizione e analisi delle digital evidence*, in Ciberspazio e Diritto, Mucchi editore, Modena, 2009.

30. *Guidelines for Evidence Collection and Archiving*, IETF, 2002. Il documento fornisce indicazioni tecniche per la corretta acquisizione e conservazione delle prove digitali, basate sul principio "dell'ordine di volatilità" e sul rispetto della catena di custodia. Sul punto si v. D. Brezinski e T. Killalea https://datatracker.ietf.org/doc/html/rfc3227

31. F. Corona, *Le attività di digital forensics nel cybercrime, in Reati informatici e investigazioni digitali,* Pacini Giuridica, 2021.

32. G. Ziccardi, *Informatica giuridica*, Giuffrè, Milano, 2006.

33. E. Casey, *The value of forensic preparedness and digital-identification expertise in smart society*, in Digital investigation, 2017, 22, pp.1-2.

34. Molteplici sono le tecniche utilizzate in tale ambito, tra le più note: il data mining, il datawarehouse, il machine learning, il clustering.

può guidare le strategie investigative[35].

Allo stesso tempo, si registra un progressivo aumento quantitativo e qualitativo di minacce e attacchi informatici che hanno impatti significativi su comunità, istituzioni e imprese[36]. L'informatica ha offerto nuove opportunità anche alle organizzazioni criminali che, a fronte di eterogeneità di target e motivazioni (finanziaria, terroristica, predatoria) sfruttano la complessità delle infrastrutture informatiche e di rete, complicando le indagini e le attività relative alla *Digital forensics*[37].

Sorgenti di dati sempre più ampie ed eterogenee, architetture distribuite, ubiquità degli spazi di archiviazione, tecniche anti-forensi[38], crittografia, virtualizzazione e la diffusione dei meccanismi di anonimato sono alcuni dei numerosi ostacoli che rendono difficile sia individuare l'azione criminosa e chi l'ha compiuta sia successivamente provare il suo accadimento[39]. La pseudo-immaterialità del processo di formazione della prova rende necessaria una nuova regolamentazione della materia o l'aggiornamento delle norme preesistenti[40].

3 Indagini su dispositivi digitali

In Italia, secondo il rapporto diffuso da Eurispes[41], lo smartphone si conferma lo strumento tecnologico più diffuso: ne ha uno il 75,5% degli italiani.

Da ciò ne discende, senza dubbio, una incessante evoluzione tecnologica che risulta proiettata verso la creazione di dispositivi sempre più avanzati, le cui caratteristiche sono in costante cambiamento. «La corsa all'arricchimento delle funzioni e dei servizi ha spinto a miscelare i concetti di cellulare, modem e personal computer determinando l'attuale concetto di *smartphone*. Le ridotte dimensioni», in uno con la conseguente «portabilità di questi sistemi, nonché l'enormità delle funzioni e l'integrazione con i computer e le reti attuali» rende il dispositivo «fondamentale nelle indagini di polizia giudiziaria»[42]. È proprio con riferimento alle indagini che emergono numerosi problemi e sfide legate ai telefoni cellulari, e in particolare agli *smartphone*[43], che come pocanzi sottolineato, sono parte integrante della vita di ciascuno di noi. Questi dispositivi

35. È questo il dominio della c.d. Cyber Intelligence. In argomento G. Costabile, *Indagini digitali*, in S. Aterno, F. Cajani, G. Costabile, D. Curtotti (a cura di), *Cyberforensics e indagini digitali*, Giappichelli, 2021, pp.77 e ss.

36. Numerosi rapporti di agenzie pubbliche, organismi e aziende registrano incidenti informatici, attacchi e minacce. Tra tutti si veda ENISA Threat Landscape 2021, su enisa.europa.eu.

37. Sul punto si v. il Rapporto quadriennale di Europol SOCTA 2021 (Serious and Organised Crime Threat Assessment).

38. L'Interpol Review of Digital Evidence 2016-2019 evidenzia che le ricerche sulle tecniche di anti-forensics costituiscono appena il 2% del totale degli studi condotti nell'ambito della Digital forensics. Le tecniche anti-forensics, generalmente, si riconducono a quattro categorie: (1) occultamento dei dati che avviene mediante la crittografia, la steganografia impiegata perché non solleva il sospetto di uno scambio di informazioni, e sistemi specifici per i dati in transito quali Virtual Private Network (VPN); (2) cancellazione degli artefatti, ovvero distruzione permanente (wiping) di file, partizioni o dischi, smagnetizzazione/distruzione di supporti di memorizzazioni, cancellazione delle informazioni presenti sui registri di sistema, manipolazione dei metadati; (3) offuscamento delle tracce, tra cui manipolazione dei file di log, spoofing degli indirizzi IP, sfruttamento di reti P2P e di server proxy e infine (4) attacchi contro strumenti forensi e processi, quali metodi che contrastano il reverse engineering o attacchi all'integrità degli hash.

39. R. Brighi, *Sfide recenti e nuovi paradigmi dell'Informatica forense*, in *nuove questioni di informatica forense*, Aracne, Roma, 2022.

40. F. Berghella – R. Blaiotta, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen*. 1995, p. 2329; F. Bravo, *Crimini informatici e utilizzo dei mezzi di ricerca della prova nella conduzione delle indagini*, in *Riv. giur. polizia*, 1998, p. 711; F. Buffa, *Internet e criminalità*, Milano, 2001; C. Serra - M. Strano, *Nuove frontiere della criminalità*, Milano, 1997. M. Luberto - G. Zanetti, *Il diritto penale nell'era digitale. Caratteri, concetti e metafore*, in *Indice pen*., 2008, p. 497; O. Dominioni, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2005, p. 117.

41. L'Eurispes, Istituto di Studi Politici, Economici e Sociali, è un ente privato e opera nel campo della ricerca politica, economica e sociale, dal 1982.

42. M. Mattiucci, *Il digital forensics: dal computer al cellulare, ad internet fino all'elettronica pura*, in Sicurezza e Giustizia, n. IV/MMXI, 50.

43. «dal punto di vista della acquisizione, la differenza tra uno smartphone e un hard disk consiste nel fatto che eseguire copie forensi bit-to-bit del primo è sostanzialmente più difficile, talvolta impossibile, mentre sul secondo la pratica è ormai consolidata sia dal punto di vista tecnico sia giuridico» P. Dal Checco, Ripetibilità e Irripetibilità delle Acquisizioni Forensi tratto dagli Atti del Convegno della tavola rotonda su "Ripetibilità e irripetibilità delle acquisizioni forensi in ambito d'indagini digitali", Roma, 2016.

possono essere considerati come un vero e proprio archivio digitale che contiene una quantità enorme di dati personali[44]. Tra questi, possiamo trovare messaggi di testo, conversazioni su app di messaggistica istantanea[45], foto, video, documenti e perfino informazioni sensibili come password e credenziali bancarie.

Ogni sistema informatico è dotato di una ampia memoria, che non solo archivia i dati utilizzati in modo ricorrente, ma registra anche una molteplicità di informazioni relative a tutte le operazioni che l'utente ha svolto nel corso del suo utilizzo[46]. A tal proposito, grazie alla sua connettività, un cellulare raccoglie continuamente dati sulla posizione dell'utente, attraverso il GPS, le reti Wi-Fi e il Bluetooth. Di conseguenza, l'accesso non autorizzato al dispositivo o l'uso improprio delle informazioni può portare ad una violazione della riservatezza personale, e nei casi più gravi al furto d'identità, alla truffa o alla diffamazione.

Tuttavia, non si può eludere un riferimento alla forma più evoluta di cellulare: il criptofonino, «*non plus ultra* offerto oggi dalla scienza e dalla tecnica in fatto di segretezza e di sicurezza delle comunicazioni»[47]. Sotto il profilo tecnico, tale dispositivo, seppure si presenti come un comune *smartphone,* è progettato per «fornire comunicazioni sicure e proteggere da *hacking* e sorveglianza»[48], attraverso modifiche strutturali, sia nella componente *software*, sia nella componente *hardware*. In particolar modo, il criptofonino è programmato per essere inaccessibile al captatore informatico, poiché sono disattivati i servizi Google, il sistema Bluetooth, il GPS, la videocamera, il microfono. Detto in altri termini, tale dispositivo chiude ogni porta di accesso al *malware*, rendendo impossibile il controllo da remoto. Non solo: le comunicazioni non utilizzano la rete tradizionale, bensì quella delle piattaforme crittografate (Sky Ecc ed Encrochat) che trasformano i messaggi – in assenza delle c.d. chiavi di cifratura – in mere stringhe numeriche prive di qualsiasi significato. Ed ancora, tali messaggi si eliminano automaticamente ed è finanche possibile la cancellazione di tutto il contenuto del dispositivo, previo inserimento di una specifica password[49].

4 Hardware, software e sistemi operativi dei dispositivi mobili

Secondo il National Institute of Standards and Technology (NIST) nel mercato della telefonia cellulare convivono almeno tre categorie di device[50]:

- ***Basic Phone***: velocità di calcolo e memoria limitata; dotato di uno schermo in scala di grigi, privo di fotocamera e di scheda di memoria aggiuntiva, senza la possibilità di connettersi ad Internet per la navigazione web e l'invio di posta elettronica;

44. Il regolamento 2016/679, c.d. GDPR, è entrato in vigore il 24.05.2016 e divenuto definitivamente applicabile in via diretta in tutti gli Stati membri il 25.05.2018. Al centro della riforma si colloca l'obiettivo di rafforzare la protezione dei dati personali, con una forte attenzione alla dimensione personalistica e individuale, M. Bassini, *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in Quad. cost., settembre 2016.

45. Tra cui WhatsApp, Messenger, Telegram o di profili/pagine dei c.d. social network (Facebook, Instagram, Twitter).

46. L. Cuomo, *La prova digitale*, in G.Canzio - L.Luparia (a cura di) *Prova scientifica e processo penale*, CEDAM, 2017.

47. Così, L. Ludovici, *I criptofonini: sistemi informatici criptati e serverocculti,* in *Penale DP*, Rivista, 2023, p. 417. Sul tema anche, W. Nocerino, *L'acquisizione della messaggistica su sistemi criptati: intercettazioni o prova documentale?*, in *Cass. pen*., 2023, p. 2786.

48. D. Curtotti, V. Rizzi, W. Nocerino, A.M. Russitto, G. Giliberti. G. Scarpa, *Piattaforme criptate e prova penale*, in *Sistema penale*, Rivista, 2023, n. 6, p. 176. Si tratta, più precisamente, di dispositivi configurati come telefoni aziendali che presentano le medesime sembianze dei devices tradizionali, ma che sono dotati di importanti sistemi di crittografia e cifratura che li rendono invulnerabili. Pertanto, le comunicazioni in entrata e in uscita sono sempre crittografate end-to-end e vengono trasmesse su un canale crittografato per proteggere ulteriormente le informazioni.

49. Di recente la Corte di cassazione si è confrontata con la tematica v. Cass., sez. VI, 15 aprile 2023, n. 16347, in *Penale DP*, (web), 23 giugno 2023, con nota di L. Filippi, *Criptofonini e diritto di difesa*. Nel caso di specie, l'azienda canadese Sky Global aveva creato una piattaforma di messaggistica elettronica protetta da un programma di crittografia denominato Sky ECC. La Sky Global forniva ai suoi clienti dispositivi telefonici nei quali erano disabilitate le funzioni di Google, oltre al GPS, microfoni, fotocamere, che permettevano di inviare e ricevere messaggi crittografati che si eliminavano automaticamente entro trenta secondi dopo la ricezione o 48 ore dopo l'invio in caso di dispositivo non raggiungibile. Era inoltre disponibile una funzione c.d. "panico" che consentiva la cancellazione del contenuto del dispositivo. Per un excursus della giurisprudenza sul tema, Cass., sez. IV, 18 aprile 2023, n. 16347, in C.E.D. Cass., n. 284563; Cass., sez. I, 13 ottobre 2022, n. 6364, ivi, n. 283998 e in Cass. pen., 2023, p. 1432; Cass., sez. IV, 7 settembre 2022, n. 32915, in www.giurisprudenzapenale.it.

50. M. Iaselli, *Investigazioni digitali*, Giuffrè Francis Lefebvre, 2020.

- ***Advanced Phone***: velocità di calcolo e memoria superiore, dotato di uno schermo in scala di colore, equipaggiato con fotocamera a bassa risoluzione; dotato di alloggiamento per schede di memoria aggiuntive, collegabile al computer tramite cavo, infrarosso o Bluetooth, in grado di collegarsi a Internet a velocità limitata per la navigazione Wap e l'invio e la ricezione di posta elettronica;
- ***Smart Phone*:** elevata capacità di calcolo e di memoria; dotato di uno schermo a colori reali ed equipaggiato con fotocamera ad alta risoluzione in grado di eseguire filmati; dotato della possibilità di contenere memorie di massa o rimovibili aggiuntive ad alta capacità; agenda collegabile a un computer, tramite cavo, infrarosso, Bluetooth e Wi-Fi; collegamento a Internet ad alta velocità per la navigazione web, l'invio e la ricezione di posta elettronica e l'instant messaging.

I sistemi operativi dei moderni dispositivi mobili possono essere suddivisi in tre categorie principali:

- Con licenza: un esempio di sistema operativo basato su licenza è la piattaforma Windows 10 Mobile. Qualsiasi azienda che produce hardware mobile può installare Windows Mobile come licenza e venderlo unitamente al telefono cellulare. L'utente finisce per pagare la licenza direttamente o indirettamente. Oggi, i sistemi operativi con licenza sono meno comuni rispetto alle altre due categorie.
- Proprietario: iOS: è il secondo sistema operativo più utilizzato, sviluppato da Apple esclusivamente per i propri dispositivi. L'aspetto vincente di iOS si basa sul concetto di sviluppo software che avviene di pari passo con l'avanzamento dell'hardware Apple, creando così un sistema complessivo molto efficiente. Questo sistema operativo presenta diversi vantaggi tra cui: velocità, sicurezza e aggiornamenti mirati. D'altro canto, questo ecosistema chiuso comporta la riduzione di possibilità di personalizzazione da parte dell'utente, lo scaricamento di App solo dallo store ufficiale e prezzi che non rendono il dispositivo alla portata di tutti.
- Fonte aperta: Android: è il sistema operativo di proprietà di Google, nonché il più usato al mondo (lo ritroviamo infatti installato sulla maggior parte degli smartphone). Nasce come open source, aspetto che ha contribuito alla sua diffusione. La personalizzazione, vantaggio principale, è molto apprezzata sia da parte dei produttori di smartphone, sia dagli utenti finali, perché lascia libertà di utilizzo a chi si interfaccia con il device[51].

5 Tracce digitali nei dispositivi mobili

La crescente diffusione e funzionalità dei dispositivi mobili ha avuto un impatto diretto sulle tecniche di analisi forense. In quest'epoca, dove i dispositivi mobili sono una parte essenziale della vita quotidiana e con l'immensa quantità di informazioni che questi dispositivi contengono, il settore della *mobile forensics*[52] è cresciuto enormemente per rispondere alle sfide poste dall'innovazione tecnologica.

«Prima degli smartphone i cellulari erano molto semplici e quasi tutto si trovava sulla scheda SIM. Poi si è passati ai cellulari con memoria e un numero sempre crescente di informazioni e contenuti (come, ad esempio, gli sms) sono migrati nella memoria del dispositivo. Il passo successivo è stata la diffusione delle fotocamere sui cellulari e infine si è arrivati agli *smartphone*, che da un punto di vista tecnico sono più simili ai computer che ai telefoni precedenti»[53]. Il moderno dispositivo elettronico ha, così, perso la sua caratteristica di mero strumento comunicativo, diventando un nuovo mondo, nel quale la persona, nello svolgere le più disparate attività (lavoro, ricerca, svago), produce dati.

51. Tecnologie dell'informazione e della comunicazione (ITS)

    https://www.itsictpiemonte.it/news/differenze-tra-android-e-ios/

52. La *mobile forensics* analizza anche il sistema operativo e le caratteristiche generali dello *smartphone* (IOS di Apple, Android di Google, Windows di Microsoft), informazioni essenziali per creare la c.d. copia forense. La mobile forensics rientra, dunque, nella più ampia categoria della digital forensics scienza che studia le metodologie investigative e le procedure per acquisire le prove digitali per finalità investigative; sul punto E. Casey, *Digital Evidence and Computer Crime. Forensics science, computers and the Internet, Elsevier*, 2004, p. 1; A. Ghirardini, G. Faggioli, *Computer Forensics*, Giappichelli, 2007; L. Luparia, G. Ziccardi, *Investigazione penale*, cit., p. 5; L. Stilo, *Computer forensics. Il volto digitale*.

53. Nanni Bassetti, segretario dell'Osservatorio nazionale sull'informatica forense (ONIF).

Le tracce digitali rinvenibili sui dispositivi mobili possono essere suddivise in tre categorie principali: dati di comunicazione, file multimediali e altri tipi di dati[54]; la combinazione di informazioni estratte da ciascuna di queste categorie consente di ottenere un quadro dettagliato della "storia digitale" di un individuo.

Tenendo conto della classificazione contenuta nelle linee-guida da ultimo predisposte dall'Interpol (Global Guidelines for Digital Forensics Laboratories), il reperimento potrà concernere[55]:

a) *cronologia delle chiamate*. La cronologia delle chiamate fornisce informazioni sulle attività di chiamata intraprese prima dell'acquisizione del dispositivo. L'analisi delle chiamate in entrata, in uscita e perse, inclusi l'ora e la durata, può consentire una verifica indiretta sulle azioni compiute dal proprietario del dispositivo stesso. Al fine di salvaguardare quantomeno la libertà e la segretezza delle comunicazioni, viene sempre vietata la conservazione del contenuto comunicativo[56]. È quindi consentita la conservazione dei soli dati esterni alle comunicazioni, quali numero telefonico del chiamante, identificativo dell'utente, dati necessari per individuare la data, l'ora e la durata di una comunicazione, data e ora del log-in e del log-off, ecc[57].

b) *elenco dei contatti*. L'elenco contatti non fornisce solo i nomi dei contatti, ma potenzialmente anche il numero di casa, il numero di cellulare e il numero di lavoro o l'eventuale e-mail del contatto medesimo. Alcuni dispositivi smartphone memorizzano anche un'immagine del contatto nell'elenco che può aiutare a identificare un determinato individuo. Le informazioni memorizzate in questo spazio del dispositivo, oltre a illustrare uno spaccato delle relazioni sociali e lavorative del suo proprietario, potrebbero contenere dati ulteriori e particolarmente significativi (molte persone, proprio nell'elenco dei contatti, memorizzano password);

c) *messaggi di testo ed e-mail*. A differenza della cronologia delle chiamate e dell'elenco contatti, che forniscono informazioni indirette, i messaggi di testo e le e-mail forniscono informazioni esplicite che, pertanto, possono risultare particolarmente utili ai fini dell'accertamento;

54. M. Iaselli, *Investigazioni digitali*, Giuffrè Francis Lefebvre, 2020.

55. M. Iaselli, *Investigazioni digitali*, Giuffrè Francis Lefebvre, 2020.

56. In tema, cfr. Corte cost. 11 marzo 1993, n. 81, nonché N. GALLO, *L'acquisizione del traffico telefonico nelle indagini di polizia*, in Riv. di polizia, II, 2008, p. 73 ss.

57. Più specificamente, le categorie di dati che possono essere conservate coincidono con quelle indicate all'art. 5 dell'abrogata direttiva 2006/24/CE. Si tratta anzitutto dei «a) dati necessari per rintracciare e identificare la fonte di una comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile: i) numero telefonico chiamante; ii) nome e indirizzo dell'abbonato o dell'utente registrato; 2) per l'accesso Internet, posta elettronica su Internet e telefonia via Internet: i) identificativo/i dell'utente; ii) identificativo dell'utente e numero telefonico assegnati a ogni comunicazione sulla rete telefonica pubblica; iii) nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati assegnati l'indirizzo di protocollo Internet (IP), un identificativo di utente o un numero telefonico; b) i dati necessari per rintracciare e identificare la destinazione di una comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile: i) numero/i digitato/i (il numero o i numeri chiamati) e, nei casi che comportano servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero o i numeri a cui la chiamata è trasmessa; ii) nome/i e indirizzo/i dell'abbonato/i o dell'utente/i registrato/i; 2) per la posta elettronica su Internet e la telefonia via *Internet*: i) identificativo dell'utente o numero telefonico del/dei presunto/i destinatario/i di una chiamata telefonica via Internet; ii) nome/i e indirizzo/i dell'abbonato/i o dell'utente/i registrato/i e identificativo del presunto destinatario della comunicazione; c) i dati necessari per determinare la data, l'ora e la durata di una comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile, data e ora dell'inizio e della fine della comunicazione; 2) per l'accesso *Internet*, la posta elettronica via Internet e la telefonia via Internet: i) data e ora del *log-in* e del *log-off* del servizio di accesso Internet sulla base di un determinato fuso orario, unitamente all'indirizzo *IP*, dinamico o statico, assegnato dal fornitore di accesso Internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato; ii) data e ora del *log-in* e del *log-off* del servizio di posta elettronica su *Internet* o del servizio di telefonia via *Internet* sulla base di un determinato fuso orario; d) i dati necessari per determinare il tipo di comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile: il servizio telefonico utilizzato; 2) per la posta elettronica Internet e la telefonia *Internet*: il servizio *Internet* utilizzato; e) i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature: 1) per la telefonia di rete fissa, numeri telefonici chiamanti e chiamati; 2) per la telefonia mobile: i) numeri telefonici chiamanti e chiamati; ii) *International Mobile Subscriber Identity* (IMSI) del chiamante; iii) *International Mobile Equipment Identity* (IMEI) del chiamante; iv) l'IMSI del chiamato; v) l'IMEI del chiamato; vi) nel caso dei servizi prepagati anonimi, la data e l'ora dell'attivazione iniziale della carta e l'etichetta di ubicazione (*Cell ID*) dalla quale è stata effettuata l'attivazione; 3) per l'accesso *Internet*, la posta elettronica su *Internet* e la telefonia via *Internet*: i) numero telefonico chiamante per l'accesso commutato (*dial-up access*); ii) *digital subscriber line* (DSL) o un altro identificatore finale di chi è all'origine della comunicazione; f) i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile: 1) etichetta di ubicazione (Cell ID) all'inizio della comunicazione; 2) dati per identificare l'ubicazione geografica delle cellule facendo riferimento alle loro etichette di ubicazione (Cell ID) nel periodo in cui vengono conservati i dati sulle comunicazioni».

d) *file multimediali*. I file multimediali, come immagini, video e file audio, possiedono una potenzialità probatoria notevole; si pensi, ad esempio, alla centralità, ai fini della ricostruzione del fatto, di un video contenente le immagini di una aggressione; o, ancora, alla importanza di un audio contenente la voce di una persona da identificare.

Inoltre, molti dispositivi smartphone, come iPhone, incorporano le coordinate GPS della posizione nei metadati denominati Exif (*Exchangeable File Format*) delle immagini. Altre informazioni incorporate nei dati Exif possono includere il marchio dello smartphone, la data e l'ora in cui sono state scattate le foto, nonché l'eventuale software utilizzato per modificare l'immagine. Tutte informazioni preziose sulle attività del proprietario del dispositivo;

e) *cronologia di navigazione in Internet e ricerca di parole chiave*. La cronologia di navigazione in Internet e le ricerche di parole chiave effettuate nel dispositivo *smartphone* forniscono una panoramica dettagliata e generale delle attività compiute in Internet e delle abitudini di navigazione del proprietario, come i siti web visitati o comunque preferiti dell'utente. Si tratta di informazioni particolarmente preziose ai fini della profilazione dell'utente;

f) *registri di chat e app di messaggistica*. Particolarmente utili possono risultare le informazioni acquisibili dalle diverse applicazioni di chat e app di messaggistica (ad esempio, WhatsApp, Telegram, Skype, Line, Weebo, WeChat, QQ, Windows Live Messenger, Google Talk e BlackBerry Messenger). Vengono in rilievo, in primo luogo, i registri della chat, in relazione ai quali, peraltro, è possibile eseguire il backup nel cloud o nell'archiviazione locale come un computer; in questi casi, la relativa ulteriore analisi può essere utile per ottenere più dati. Inoltre, rilevano le chiamate eseguite attraverso tali applicazioni; le app di messaggistica, infatti, possono anche offrire il servizio VoIP (*Voice over IP*) che consente al proprietario dello smartphone di comunicare utilizzando il protocollo IP, senza lasciare un record nella cronologia delle chiamate del dispositivo;

g) *account dei social network*. Gli account dei social network, come Instagram, Facebook, Twitter, memorizzano le credenziali dell'utente nel dispositivo stesso. Queste credenziali sono particolarmente preziose, potendo essere utilizzate per ottenere l'accesso all'account dei social media sospetti, consentendo l'estrazione dei dati dal dispositivo: elenchi di contatti, messaggi tra singoli e gruppi, immagini, video, attività dell'utente e così via;

h) *connessioni (rete mobile, Wi-Fi, Bluetooth).* Anche questi aspetti possono fornire una panoramica delle attività di rete svolte dal dispositivo smartphone del proprietario. La rete mobile fornirà un'immagine del paese o della regione in cui il proprietario ha effettuato il roaming. Il Wi-Fi fornirà un'immagine della rete locale (LAN) a cui lo smartphone è connesso. Le connessioni Bluetooth forniranno informazioni sui soprannomi dei dispositivi che erano collegati con il proprietario dello smartphone.

6 Dislocazione dei dati e aree di interesse investigativo

Nel provare ad entrare nel dispositivo elettronico in esame, qualche puntualizzazione tecnica appare imprescindibile in ragione della pluralità non solo di dati memorizzabili sul dispositivo, ma anche delle distinte memorie che sono deputate a custodirli. Più nel dettaglio, i dati possono essere acquisiti dalla c.d. scheda SIM *(Subscriber Identity module),* dalla memoria esterna (ad esempio, *Secure Digital Card o MultiMedia*

Card), dalla memoria interna, dalle App, dai Cloud[58] e, infine, dal gestore dei servizi[59].

La scheda SIM è una componente rimovibile del dispositivo da cui è possibile ricavare le principali informazioni relative al sottoscrittore del servizio mobile, tra cui il codice ICCID (*Integrated Circuit Card Identification*) che identifica univocamente la SIM; il codice IMSI (*International Mobile Subscriber Identity*), che identifica il numero univoco dell'utente all'interno della rete del suo operatore; o ancora, le informazioni sulla localizzazione relative alle comunicazioni vocali (*Location Area Information*) o alle trasmissioni di dati (*Routing Area Information*).

La sicurezza della SIM, nonché i diritti di accesso dell'utente, vengono garantiti dall'attribuzione di un codice di 4-8 cifre denominato *Personale Identification Number* (PIN), che sempre più spesso è associato a meccanismi di blocco dello schermo attraverso sequenze grafiche o numeriche. L'attivazione del PIN o degli ulteriori meccanismi di sicurezza condiziona fortemente l'accesso ai dati e la scelta delle modalità operative più idonee alla loro acquisizione; basti pensare, infatti, l'inserimento di un codice PIN errato per tre volte manda usualmente la scheda in blocco temporaneo e rende necessario inserire, o richiedere al Network Service Provider, un codice PUK (*Personal Unlocking Key*), il cui inserimento errato per dieci volte manda la SIM in blocco definitivo. Per quanto riguarda l'estrazione delle informazioni dalla scheda, generalmente viene effettuata attraverso l'ausilio di un lettore di SIM Card, previa rimozione della SIM dall'alloggiamento nel telefono.

I telefoni cellulari avanzati e gli *smartphone* dispongono di slot per ospitare memorie aggiuntive rimovibili che espandono considerevolmente la memoria del dispositivo e garantiscono un ampliamento notevole dello spazio di salvataggio dei dati. Si tratta di schede generalmente utilizzate per la memorizzazione di file multimediali, come ad esempio audio, video, immagini e documenti che, anche in ragione delle dimensioni ridotte, possono costituire uno strumento privilegiato per l'occultamento, il trasferimento e lo stoccaggio di dati. Durante la fase di analisi, l'operatore dovrà prestare la massima attenzione all'identificazione del posizionamento di queste memorie all'interno del dispositivo[60].

L'estrazione delle informazioni può essere effettuata, ad esempio, mediante dispositivi quali il *write blocker*[61], che permettono l'accesso ai dati presenti su un supporto di memorizzazione di dati digitali, prevenendo scritture e alterazioni.

Lo spazio di maggiore interesse, e di maggiore difficoltà nella *mobile forensics*, è rappresentato dalla memoria interna di dispositivo. La memoria interna rappresenta il luogo ove risiede il *software* del telefono e, disponendo di un più vasto spazio di memoria rispetto alla scheda SIM, consente di custodire maggiori informazioni, quali, ad esempio, le impostazioni del telefono, la rubrica dei contatti, gli SMS inviati e ricevuti, le App scaricate (la più comune è WhatsApp), il registro delle chiamate[62]. Bisogna considerare, infatti, che i *mobile devices* contengono tipologie di memoria che possiedono caratteristiche differenti in termini di volatilità o non volatilità del contenuto[63].

---

58. Il termine *Cloud* si riferisce ad un *server* a cui si accede tramite Internet che consente agli utenti di accedere a determinati file ed applicazioni (ad esempio Dropbox, Google Drive, Google Foto) da ogni dispositivo, perché l'elaborazione e l'archiviazione dei dati non avviene all'interno del dispositivo, bensì nel c.d. *cyber* spazio, un *datacenter* amministrato da vari gestori, generalmente localizzato all'estero. Il sistema *Cloud* consente ad ogni utente di accedere al proprio account utilizzando qualsiasi dispositivo telefonico (ma anche dal computer, tablet). L'ambito di ricerca dei dati non è più quello del dispositivo elettronico oggetto di ispezione, perquisizione o sequestro, ma lo spazio *cyber* gestito da un *provider*. La disciplina che studia le metodologie per l'analisi forense dei sistemi *cloud* è denominata *cloud forensics*. Per un approfondimento si rimanda a G. Costabile, *Le indagini digitali*, in *AA.VV*., *Cyber forensics e indagini digitali*, cit., p. 61; L. C. Hopper, B. Martin, K.K. Raymond Choo, *Cloud Computing and Its Implications for Cybercrime Investigations in Australia, in Computer Law & Security Review*, 2013, vol. 29, p. 2; A. Pichan, M. Lazarescu, S.T. SOH, Cloud Forensics: Technical Challanges, Solutions and Corporative Analysis, in Digital investigation, 2015, vol. 13, p. 38.

59. Il riferimento è ai dati c.d. esteriori delle comunicazioni racchiusi nei tabulati di traffico telefonico e telematico.

60. S. Epifani, *Analisi di telefoni cellulari in ambito giuridico, relazione all'Incontro studi sul tema «Scienze e processo penale»,* Roma, 27-29 giugno 2011, in www.csm.it

61. L'estrazione e l'analisi sarà compiuta attraverso dei dispositivi come il write blocker che consentono l'accesso ai dati digitali del supporto di memorizzazione, prevenendo alterazioni e scritture; per un approfondimento sulla Mobile Forensisc Analisys, M. Tonellotto, *Evidenza informatica, computer forensics e best practices*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, 2014, p. 93.

62. O. Murro, *Lo smartphone come fonte di prova. Dal sequestro del dispositivo all'analisi dei dati*, CEDAM, 2024.

63. S. Calabrò, *Mobile device and mobile cloud computing forensics*, Torino, 2016.

Gli strumenti e i metodi a disposizione per l'analisi delle memorie interne dipendono dal tipo di sistema operativo utilizzato dal dispositivo mobile. In linea generale l'analisi della memoria interna viene effettuata attraverso un personal computer su cui sia installato un *software* di estrazione dei dati (*software di backup* del dispositivo o *software* dedicato per la *mobile forensics*) o attraverso un dispositivo *hardware* dedicato; in entrambi i casi è necessario assicurare una connessione tra il dispositivo e lo strumento di acquisizione[64].

La connessione, a seconda del modello, si potrà realizzare via cavo, tramite infrarossi o via onde radio Bluetooth; è preferibile procedere con la connessione via cavo perché, oltre ad essere più sicura ed affidabile, risulta avere un minore impatto sui dati; laddove non sia disponibile il cavo di connessione per il modello da analizzare, si consiglia di utilizzare una connessione a infrarosso e, solo in via di extrema ratio, una connessione Bluetooth, la quale genera modifiche al dispositivo durante la fase di attivazione e autenticazione della connessione[65]. Infine, vi sono i dati di traffico telefonico e telematico[66], richiesti al gestore del servizio, che possono fornire un quadro dettagliato sul flusso di comunicazione telefonica o telematica: numero chiamante e del chiamato, data, orario e durata delle conversazioni, data e orario di invio e ricezione di SMS o MMS, cronologia internet, dati localizzazione.

Sulla base di queste considerazioni, e da un punto di vista generale, si delineano due distinte procedure di approccio a seconda che il telefono sia spento o acceso[67]:

TELEFONO CELLULARE SPENTO

Effettuare una analisi esterna e documentale del telefono, anche mediante foto e video

Se il telefono contiene una SIM, rimuoverla

Se il telefono contiene una memoria rimovibile, rimuoverla

Effettuare l'analisi della SIM

Effettuare l'analisi della memoria rimovibile

Per preservare lo stato della SIM è opportuno clonarla e utilizzare la carta clonata per la successiva analisi del telefono

Ove non sia possibile effettuare un clone, utilizzare una metodologia alternativa di isolamento del telefono dalla rete

Collegare il telefono a una fonte di alimentazione fissa o portatile

Attivare la procedura di riconoscimento del telefono da parte del software prescelto

Accendere il telefono

Stabilire la connessione tra il telefono e il software

Estrarre le informazioni, utilizzando le funzionalità proprie del software in uso

TELEFONO CELLULARE ACCESO

64. S. Epifani, *Analisi di telefoni cellulari in ambito giuridico, relazione all'Incontro studi sul tema «Scienze e processo penale»*, Roma, 27-29 giugno 2011, in www.csm.it

65. Selene Giupponi, responsabile della Digital Forensics Unit presso Security Brokers, ha più volte sottolineato l'importanza di preferire connessioni via cavo nelle attività di acquisizione forense, in quanto più sicure e meno invasive per l'integrità del dato digitale.

66. Sulla recente riforma che ha modificato la disciplina dei dati c.d. esteriori alle comunicazioni si rimanda a F. Demartis, *La nuova disciplina sui tabulati: un completo adeguamento agli standard europei?*, in *Dir. pen. proc*., 2022, p. 306; F.R. Dinacci, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *Proc. pen. giust*., 2022, p. 310; nonché, volendo, O. Murro, *Dubbi di legittimità costituzionale e problemi di inquadramento sistematico della nuova disciplina dei tabulati*, in *Cass. pen*., 2022, p. 2440. Sul tema, già L. Filippi, *Il rilevamento del tracciato axe: una nuova denominazione per una vecchia indagine*, in *Giur. it*., 1999, p. 1687.

67. S. Epifani, *Analisi di telefoni cellulari in ambito giuridico, relazione all'Incontro studi sul tema «Scienze e processo penale»*, Roma, 27-29 giugno 2011, in www.csm.it

Collegare il telefono a una fonte di alimentazione fissa o portatile

Estrarre le informazioni dal telefono in ambiente schermato

Analizzare la SIM e la memoria rimovibile

In base allo scenario fin qui delineato, si può rilevare come la possibilità per gli investigatori di disporre di un ampio bacino di informazioni possa senz'altro contribuire all'efficacia investigativa[68]. Tuttavia, si tratta di capire in che modo, quando e in quale misura queste informazioni possano essere legittimamente acquisite, dato che "Ogni sequestro probatorio deve essere commisurato alle reali esigenze investigative"[69].

Da un lato, infatti, la tecnologia digitale ha ampliato le possibilità di trattamento di dati. Dall'altro lato, però, vi è il rischio che il monitoraggio delle persone si trasformi in «capitalismo della sorveglianza»[70] o schiuda scenari da *panopticon* idonei a determinare significative compressioni dei diritti fondamentali e, in fondo, un *vulnus*, alla stessa dignità dell'uomo, attraverso la reificazione di quest'ultimo, ricondotto a mero insieme di dati[71]. Per raggiungere i suoi fini, infatti, il procedimento penale si nutre di informazioni ed è "onnivoro" di conoscenza. La dimostrazione di ciò è nel codice di procedura penale e, in particolare, in tutte quelle norme che disciplinano le indagini e le prove: sia i mezzi di prova, sia i mezzi di ricerca della prova sono funzionali ad ottenere informazioni utili all'accertamento processuale e si giustificano proprio in ragione di tale scopo. Queste informazioni sono raccolte, selezionate, interconnesse e raffrontate, in palese e continua violazione del diritto alla riservatezza[72], o almeno in sua contraddizione.

Tale rischio assume contorni particolarmente concreti e problematici proprio nell'ambito giudiziario e investigativo, dove l'utilizzo delle tecnologie forensi — se prive di adeguati contrappesi normativi e giurisprudenziali — può favorire la normalizzazione di pratiche intrusive e tecniche sofisticate di sorveglianza. Anche nel settore giudiziario e investigativo, sebbene animato da finalità pubbliche legittime, l'accesso massivo ai dati rischia di contribuire alla normalizzazione di pratiche intrusive, riducendo la persona a oggetto passivo di controllo tecnologico.

Il sequestro indiscriminato dell'intero sistema informatico, in carenza di presupposti, può rivelarsi eccessivamente invasivo ed eccedente rispetto allo scopo di tutela della genuinità della prova, ledendo in tal modo i diritti fondamentali della persona che risultano protetti a livello costituzionale dalle disposizioni relative alla riservatezza, alla segretezza, al diritto di proprietà e al diritto di difesa[73].

È dunque imprescindibile, soprattutto nell'utilizzo degli strumenti di *mobile forensics*, riaffermare con forza il principio di proporzionalità e la necessità di un controllo giurisdizionale effettivo. Soltanto attraverso un uso

68. S. Signorato, *Data retention, tra diritto alla protezione dei dati personali ed esigenze di accertamento dei reati*, R. Brighi (a cura di), *Nuove questioni di informatica forense*, Aracne, Roma, 2022. Naturalmente, purché tali informazioni siano corrette e adeguatamente selezionate. Va rilevato come, con specifico riguardo al principio della correttezza nel trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, l'art. 4 direttiva (UE) 2016/680 (cd. direttiva law enforcement) preveda espressamente il principio della correttezza nel trattamento dei dati.

69. Corte Cassazione penale sez. VI 35033/2024.

70. S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, tradotto da P. Bassotti, Luiss University Press, Roma 2019.

71. Una volta che «la persona si pone come una "entità disincarnata", ne consegue l'esigenza di tutelarne il "corpo elettronico". In questi termini, si sente il bisogno di una sorta di "habeas corpus", nella forma di un "habeas data", configurabile come l'evoluzione del nucleo dal quale storicamente si è sviluppata la libertà personale». Così, L. Parlato, *Libertà della persona nell'uso delle tecnologie digitali*, in *Associazione tra gli studiosi del processo penale, Diritti della persona e nuove sfide del processo penale*, Giuffrè Francis Lefevre, Milano 2019, p. 211, nonché S. Rodotà, *Il mondo della rete. Quali vincoli, quali diritti*, Laterza, Roma 2014, p. 30.

72. Così, S. Carnevale, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, D. Negri – S. Carnevale – M. P. Addis (a cura di) *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Aracne, Roma, 2007

73. Il sequestro probatorio della memoria del persona computer di un giornalista che abbia opposto il segreto professionale è consentito soltanto ove sia ritenuta l'infondatezza del segreto e la necessità dell'acquisizione per l'indagine, anche se l'attività investigativa deve essere condotta in modo da non compromettere il diritto del professionista alla riservatezza della corrispondenza e delle proprie fonti, Cass., Sez. I, 16 febbraio 2007, n. 25755.

regolato, trasparente e consapevole delle tecnologie investigative è possibile evitare derive che, pur motivate da esigenze legittime, possano produrre effetti distorsivi sui diritti fondamentali, alimentando un ecosistema digitale in cui la sicurezza venga perseguita a scapito della libertà. L'equilibrio tra efficienza investigativa e tutela dei diritti non è solo una questione tecnica o giuridica, ma una sfida etica e culturale, che interroga la concezione stessa di cittadino e di società democratica nell'era digitale.

7 WhatsApp, E-mail e SMS: Corrispondenza o Documenti?

Una delle principali problematiche connesse alla *Digital forensics* riguarda le modalità di acquisizione, conservazione e successivo utilizzo in dibattimento delle prove digitali.

In particolare, un aspetto di grande rilievo è rappresentato dall'acquisizione e dalla valenza probatoria dei messaggi di posta elettronica e dei servizi di messaggistica istantanea, come WhatsApp. Queste forme di comunicazione, pur essendo ampiamente utilizzate nella vita quotidiana, pongono numerosi interrogativi dal punto di vista giuridico, soprattutto in relazione alla loro attendibilità, alla tutela della privacy e alla loro corretta utilizzazione nei procedimenti giudiziari.

In un primo momento, la giurisprudenza tendeva a considerare e-mail e messaggi istantanei alla stregua di semplici documenti informatici, non beneficiando così delle garanzie previste dall'art. 15 della Costituzione, il quale tutela l'inviolabilità della corrispondenza e di ogni altra forma di comunicazione. Questa interpretazione aveva conseguenze rilevanti sul piano probatorio: se considerati documenti, i messaggi potevano essere acquisiti con modalità meno rigorose, senza le particolari restrizioni previste per la corrispondenza.

Successivamente, questa questione è stata oggetto di analisi da parte della Corte Costituzionale, che ha dovuto stabilire se l'acquisizione di e-mail e messaggi di chat rientrasse o meno nel paradigma del sequestro di corrispondenza, in particolare con la sentenza n. 170 del 2023.

Un primo punto chiarito dalla Corte è la distinzione tra le intercettazioni di comunicazione o conversazioni e i sequestri di corrispondenza. In base alla giurisprudenza delle Sezioni Unite della Corte di Cassazione penale, per "intercettazione deve intendersi l'apprensione occulta, in tempo reale, del contenuto di una conversazione o di una comunicazione in corso tra due o più persone da parte di altri soggetti estranei al colloquio"[74].

Affinché vi sia intercettazione devono sussistere due condizioni. La prima è di ordine temporale: la comunicazione deve essere in corso nel momento della sua captazione da parte dell'extraneus; questa deve cogliere, cioè, la comunicazione nel suo momento "dinamico".

Diversamente, se l'acquisizione avviene quando la comunicazione è già avvenuta e si trova memorizzata su un supporto (ad esempio, una casella e-mail o una chat salvata sul telefono), si rientra nel concetto di sequestro (dunque, nel suo momento "statico").

La seconda condizione attiene alle modalità di esecuzione: l'apprensione del messaggio comunicativo da parte del terzo deve avvenire in modo occulto, ossia all'insaputa dei soggetti, tra i quali la comunicazione intercorre[75].

Partendo da questo presupposto, la Corte Costituzionale ha sottolineato che il concetto di corrispondenza va interpretato in senso ampio, includendo qualsiasi forma di comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate, attuata in modo diverso dalla conversazione in presenza. La stessa Corte ha più volte affermato che la tutela accordata dall'art. 15 Cost. prescinde dalle caratteristiche del mezzo tecnico utilizzato ai fini della trasmissione del pensiero, "aprendo così il testo costituzionale alla possibile emersione di nuovi mezzi e forme di comunicazione riservata"[76].

Da ciò ne consegue che la garanzia si estende, ad ogni altro strumento che l'evoluzione tecnologica mette a disposizione a fini comunicativi, compresi quelli elettronici e informatici. Posta elettronica e messaggi inviati

74. Corte di cassazione, sezioni unite penali, sentenza 28 maggio – 24 settembre 2003, n. 36747.

75. Corte Cost. senzt. n. 170 del 2023.

76. Corte Cost. sent. n. 2 del 2003.

tramite l'applicazione WhatsApp (appartenente ai sistemi di cosiddetta messaggistica istantanea) rientrano, dunque, a pieno titolo nella sfera di protezione dell'art. 15 Cost., apparendo del tutto assimilabili a lettere o biglietti chiusi. La riservatezza della comunicazione, in questo caso, è assicurata dal fatto che la posta elettronica viene inviata a una specifica casella di posta, accessibile solo al destinatario tramite credenziali personali; mentre i messaggii WhatsApp, vengono recapitati in modo criptato al dispositivo del destinatario, solitamente protetto da un sistema di autenticazione.

Nella stessa direzione si muove anche la giurisprudenza della Corte Europea dei Diritti dell'Uomo (CEDU), che ha riconosciuto senza incertezze come i messaggi di posta elettronica[77], gli SMS[78], e la messaggistica istantanea inviata e ricevuta tramite internet[79] rientrino pienamente nella sfera di protezione dell'art. 8 CEDU.

Un ulteriore aspetto problematico, chiarito dalla Corte Costituzionale e dalla stessa CEDU, riguarda la natura giuridica dei messaggi di posta elettronica e WhatsApp già ricevuti e letti dal destinatario, ma conservati nella memoria dei dispositivi elettronici. Il nodo centrale della questione era stabilire se tali comunicazioni, una volta recapitate e lette, perdessero la loro natura di corrispondenza.

La Corte, riprendendo un orientamento ormai consolidato, in base al quale la tutela garantita dall'art. 15 Cost. si estende anche ai dati esteriori delle comunicazioni, ossia quegli elementi che permettono di ricostruire il fatto storico della comunicazione (come l'identità del mittente e del destinatario, il momento e il luogo in cui è avvenuta); ha ritenuto che anche il sequestro di messaggi elettronici già ricevuti e conservati debba rientrare nell'ambito di protezione garantito alla corrispondenza.

La stessa CEDU ha ribadito questa impostazione, sottolineando che l'art. 8 CEDU protegge non solo la fase dinamica della comunicazione, ma anche la sua dimensione "statica"[80] . Ad oggi rimane aperta una questione di non poco conto: la Corte ha affermato che le e-mail, gli SMS, la messaggistica istantanea rientrano nell'alveo della corrispondenza "almeno fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità, in rapporto all'interesse alla riservatezza, trasformandosi in mero documento storico"[81]. Tale carattere di attualità deve presumersi fino a prova contraria. Tuttavia, non sembra esservi, ad oggi, una giurisprudenza consolidata che chiarisca quando un messaggio digitale possa definitivamente perdere la sua natura di corrispondenza per divenire un mero documento storico; questo lascia spazio ad una serie

di interrogativi: dopo quanto tempo un messaggio può considerarsi "storico? Non sarebbe opportuno adottare dei criteri chiari e oggettivi al fine di effettuare questa valutazione?

8 Affidabilità e trasparenza dei software utilizzati nella Digital Forensics

Le sfide che la modernità pone all'operatore del diritto derivano dalla diffusione esponenziale degli strumenti tecnologici e dalla loro capacità di influenzare la vita delle persone[82]. Gli apparecchi elettronici costituiscono strumenti di percezione e, al tempo stesso, di creazione dello spazio virtuale generato dalle interazioni che vengono a stabilirsi tra le macchine e gli utenti: l'informatica, unitamente alla telefonia, è diventata la piattaforma in cui viene svolta la maggior parte delle attività lavorative, sociali e personali[83]. Tuttavia, il baricentro di un

77. Corte EDU, grande camera, sentenza 5 settembre 2017, Barbulescu contro Romania, paragrafo 72; Corte EDU, sezione quarta, sentenza 3 aprile 2007, Copland contro Regno Unito, paragrafo 41.

78. Corte EDU, sezioni quinta, sentenza 17 dicembre 2020, Saber contro Norvegia, paragrafo 48.

79. Corte EDU, Grande Camera, sentenza Barbulescu, paragrafo 74.

80. Con riguardo alla posta elettronica, Corte EDU, sentenza Copland, paragrafo 44; con riguardo alla messaggistica istantanea, Corte EDU, sentenza Barbulescu, paragrafo 74; con riguardo a dati memorizzati in floppy disk, Corte EDU, sezione quinta, sentenza 22 maggio 2008, Iliya Stefanov contro Bulgaria, paragrafo 42).

81. Corte Cost. senzt. n. 170 del 2023.

82. L. Cuomo, *La prova digitale*, G. Canzio – L. Luparia (a cura di) *Prova scientifica e processo penale,* Cedam, 2017.

83. In tema v. A. Valastro, *La tutela penale delle comunicazioni intersoggettive, fra evoluzione tecnologica e nuovi modelli di responsabilità*, in *Riv. it. dir. e proc. pen*., 1999, p. 989; R. Frank, *Tutela della riservatezza e sviluppo tecnologico*, in *Giust. civ*., 1987, p. 26.; R. Galli, *Alcune note sulla «privacy» (legge n. 675 del 1996)*, in *Foro pad*., 1998, p. 121; V. Grippo, *Analisi*

processo fondato sulla prova scientifica si colloca sempre più nelle indagini preliminari, in cui il dato digitale viene di regola acquisito dalla polizia giudiziaria e successivamente analizzato da personale tecnico[84]. Il dato digitale presenta i caratteri della immaterialità e della fragilità, per cui può essere facilmente modificato o cancellato da personale non in possesso di conoscenze tecniche adeguate[85]. Per tali ragioni, l'acquisizione e la conservazione della prova informatica deve avvenire attraverso un processo volto alla manipolazione controllata dei dati, che sia in grado di fornire adeguate garanzie di integrità, autenticità e disponibilità delle informazioni[86]. Ed invero, se la libertà della persona si estende sino a ricomprendere gli oggetti che costituiscono parte fondamentale della sua esistenza, è di tutta evidenza come lo *smartphone* divenga un luogo di tutela, «una sorta di *habeas corpus*, nella forma di un *habeas data*»[87], in linea con l'evoluzione del nucleo centrale della libertà personale[88]. L'*habeas corpus*, infatti, è l'espressione del diritto all'intangibilità della persona; nel contempo, l'*habeas data* rappresenta il diritto del singolo di avere il controllo sui propri dati personali, compresa la facoltà di impedirne la conoscenza e la circolazione[89].

Per Vittorio Frosini «l'informazione sul conto di una persona è una forma di "ispezione personale", che viene compiuta in forma morale e non fisica, e che perciò ricade sotto il divieto, stabilito dall'art. 13 della stessa Costituzione, di restrizioni della libertà personale»[90]. Era la metà degli anni Settanta e la sentenza[91] "*Soraya*" introduceva per via giurisprudenziale il diritto alla riservatezza nell'ordinamento italiano, ma oggi il diritto alla propria identità informatica è scomparso. Come mai? A nulla è valso l'affannato ed operoso lavorìo di tante grandi menti giuridiche, non è né l'intelligenza né l'impegno che sono mancati, bensì la competenza: un'adeguata visione sul mondo delle tecniche dell'informazione, una formazione giuritecnica[92].

---

dei dati personali presenti su Internet. La legge n. 675/96 e le reti telematiche, in *Riv. critica dir. priv*., 1997, p. 639; V. Librando, *La tutela della riservatezza nello sviluppo tecnologico*, in *Dir. inf. e informatica*, 1987, p. 487; L. Cuomo - B. Izzi, *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico*, in *Cass. pen*., 2002, p.1018. Nel corso degli anni si è modificato il rapporto "uomo-computer", considerato che, se in origine era effettivamente un mezzo per svolgere una attività professionale, attualmente è un vero e proprio ambito spaziale all'interno del quale l'individuo proietta tutta la sua personalità. È allora facile immaginare che a breve non avrà più senso distinguere tra domicilio comune e domicilio informatico, nel senso che quest'ultimo si avvicinerà come contenuti sempre più al primo, con la conseguenza che i criteri da seguire per apprestare adeguata protezione saranno meno incerti rispetto a quanto accade oggi» P. Galdieri, *Il domicilio informatico: l'interpretazione dell'art. 615-ter cod. pen. tra ragioni di carattere sistematico e forzature*, in *Diritto inf.,* 2013, p. 88 ss.).

84. L. Cuomo, *La prova digitale*, cit.

85. Le difficoltà operative sono legate alla natura stessa della scena del crimine digitale, localizzata tra i polpastrelli dell'autore e la tastiera, tra i suoi occhi e le emissioni elettromagnetiche del «monitor». Senza contare, poi, le innumerevoli possibilità di anonimizzazione e di sostituzione dell'identità altrui offerte dall'ambiente digitale, L. Marafioti, *Digital evidence e processo penale*, in *Cass. pen*., 2011, p. 4509); S. Aterno - F. Cajani - G. Costabile - M. Mattiucci - G. Mazzaraco (a cura di), *Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Experta, Forli, 2011, p. 411.

86. G. Costabile, *Computer forensics e informatica investigativa alla luce della legge n. 48 del 2008, in Ciberspazio e diritto*, 2010, p. 465 ss.; L. Lupária - G. Ziccardi, *Investigazione penale e tecnologia informatica*, 2007, Giuffrè, Milano, p. 136.

87. L. Parlato, *Libertà della persona nell'uso delle tecnologie*, in *Processo Penale e Giustizia*, 2020, cit., p. 295. Lo *Habeas Data* fu il tema dell'intervento di V. Frosini "*La protezione della riservatezza nella società informatica" tenuto al seminario su "Privacy e banche dei dati: aspetti giuridici e sociali"*, organizzato dall'Associazione di politica e cultura Il Mulino in collaborazione con l'IBM Italia (Roma, 25 febbraio 1981), poi pubblicato in diverse sedi, vedi: V. Frosini, *La protezione della riservatezza nella società informatica*, in N. Matteucci (a cura di),"*Privacy e banche dei dati"*, Bologna, Il Mulino, 1981, 37 ss; ID., in *questa Rivista*, 1981, n. 1, p. 5 ss.; ID., *Informatica diritto e società*, II ed., Milano, Giuffrè, 1992, p. 173 ss. Unitamente allo *Habeas Data* la riflessione di Frosini si rivolge alla libertà ed alla identità informatiche, cfr. F. Riccobono, *La filosofia del diritto di Vittorio Frosini dalla morfologia della prassi all'informatica giuridi*ca, in D. Charalambis, C. Papacharalambous (Hrsg. von), *Jus, ars, philosophia et historia. Festschrift für Johannes Strangas*, Nomos, Baden-Baden 2017, p. 696 ss.

88. Sul tema si rimanda a S. Rodotà, *Il mondo nella rete. Quali vincoli, quali diritti*, Laterza, 2014, p. 102.

89. Per un approfondimento, S. Rodotà, *Libertà personale. Vecchi e nuovi nemici*, M. Bovero (a cura di) *in Quale libertà. Dizionario minimo contro i falsi liberali*, Laterza, 2004, p. 52. Sul rapporto tra l'habeas data con la dimensione statica e dinamica della privacy, S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, p. 75. Affronta il tema dell'habeas corpus in relazione all'art. 13 Cost., M. Daniele, Habeas corpus. Manipolazioni di una garanzia, Giappichelli, 2017, p. 29.

90. V. Frosini, *I calcolatori elettronici e il nuovo mondo civile, in «Rivista internazionale di filosofia del diritto», 4, 1973, p. 704 ss.; Id., La giuritecnica: problemi e proposte, in «Informatica e diritto», 1, 1975, p. 26 ss., Id., Informatica diritto e società, Giuffrè, Milano, 1988; Id., La giuritecnica: problemi e proposte, in «Amministrazione e politica», 3, 1976, p.187 ss.*

91. Cass. 27 maggio 1975, n. 2129, detta "sentenza Soraya", in «Foro Italiano», 1976, pt. I, c. 2895 ss.

92. Così F. Romeo, *Habeas Data*, la forza normativa di un'idea, D'Avack, Faralli, T.E. Frosini, Jellamo, Andrini, Riccobono, Limone,

Frosini introduce il nuovo importante concetto di identità informatica: «All'arbitrio di chi detiene abusivamente in prigionia una persona, corrisponde infatti l'arbitrio di chi detiene, senza la dovuta autorizzazione, quella che si vorrebbe chiamare la "identità informatica" di una persona, cioè l'insieme dei dati, che consentono di ricomporre l'immagine morale della sua personalità (della quale possono entrare a far parte anche elementi d'ordine biologico, come predisposizioni per malattie ereditarie, malformazioni fisiche, tare psichiche e turbe sessuali); i quali dati, raccolti, memorizzati ed elaborati in un calcolatore elettronico, diventano – a differenza di quelli riportati su una comune scheda segnaletica – immediatamente accessibili e diffusibili»[93]. «Con enfasi riduzionista, per molti versi pericolosa, si dice che "noi siamo le nostre informazioni". La nostra identità viene così affidata al modo in cui queste informazioni vengono trattate, collegate, fatte circolare»[94].

La *Digital forensics* rappresenta un settore in continua evoluzione, in cui l'equilibrio tra efficienza investigativa e garanzia della trasparenza è cruciale per assicurare processi equi e attendibili. L'uso di *software* proprietari nella *Digital forensics* solleva numerose questioni di affidabilità e trasparenza, con dirette implicazioni sul valore probatorio delle evidenze digitali. La dipendenza da strumenti il cui codice sorgente non è accessibile, apre o dovrebbe aprire un dibattito sulla validità delle prove acquisite, sulle modalità di analisi e sulla riproducibilità dei risultati. L'uso di *software* forensi proprietari è ampiamente diffuso per la loro capacità di offrire strumenti avanzati e funzionalità specifiche, spesso riconosciute dagli standard internazionali e accettate nei procedimenti giudiziari. Tuttavia, la natura chiusa di questi strumenti implica alcune criticità: in primo luogo la mancanza di trasparenza, l'impossibilità di accedere al codice sorgente rende difficile verificare come i dati vengano acquisiti e analizzati. Inoltre, altro problema soggiace con riferimento all'affidabilità delle prove, infatti, senza un controllo indipendente, non si può escludere la presenza di errori o manipolazioni nei *software.*

Per ultimo, vi è la dipendenza dal produttore del *software* stesso; gli aggiornamenti e le metodologie utilizzate sono nelle mani delle aziende che sviluppano questi strumenti, senza un controllo esterno da parte della comunità scientifica. Da ciò derivano una serie di interrogativi:

a. Le prove ottenute sono attendibili se non si conosce il funzionamento del *software*?

b. I dati acquisiti sono realmente inalterabili e verificabili?

c. In che modo la mancanza di accesso al codice sorgente influisce sulla riproducibilità delle analisi?

d. Le decisioni giurisprudenziali hanno considerato il problema dell'uso di *software* proprietari?

Questi sono alcuni dei molteplici interrogativi di cui ci si dovrebbe preoccupare anche in considerazione dell'assenza di una giurisprudenza consolidata in materia[95].

Una possibile soluzione potrebbe essere l'adozione di software open source, che garantirebbero un controllo indipendente e una maggiore riproducibilità delle analisi forensi. Tra i vantaggi principali degli strumenti *open source* si evidenziano: verificabilità del codice (chiunque può analizzarne il funzionamento e verificare l'affidabilità dei risultati), revisione continua da parte della comunità accademica e forense e infine, l'indipendenza dai produttori commerciali.

Le linee guida internazionali rappresentano il punto di partenza essenziale per garantire che le indagini digitali siano condotte in modo affidabile, riproducibile e trasparente. Standard come l'ISO/IEC 27037 (che fornisce linee guida per la gestione delle prove digitali) e le raccomandazioni del National Institute of Standards and

Romeo, Caridi, Ciacci, Punzi (a cura di) in *Vittorio Frosini: una coscienza giuridica aperta al futuro, Rivista internazionale di filosofia del diritto,* Giuffrè Francis Lefebvre, 2019.

93. V. Frosini, *La protezione della riservatezza nella società informatica*, cit., p. 44.

94. S. Rodotà, Una scommessa impegnativa sul terreno dei nuovi diritti, *InterLex Diritto Teconolgia e Informazione,* 2002, http://www.interlex.it/675/rodota6.htm.

95. Nel quadro del progetto PRIN «Prova e processo informatizzato», l'autore come parte del gruppo di ricerca, ha tentato di sollevare presso le autorità inquirenti, la polizia scientifica e i reparti di polizia cibernetica alcune delle questioni sopra delineate, ponendo interrogativi centrati sull'uso di *software* proprietari in ambito forense, sulla trasparenza metodologica e sull'indipendenza dell'analisi tecnica. Nonostante gli sforzi, tale attività di confronto si è conclusa senza riscontri sostanziali, confermando la necessità di un dibattito più aperto e consapevole tra operatori del diritto, tecnici e istituzioni.

Technology (NIST) sono fondamentali per orientare la selezione degli strumenti da utilizzare, siano essi software proprietari o open source.

Tali standard stabiliscono che, indipendentemente dal tipo di software utilizzato, le procedure di acquisizione, analisi e gestione delle prove devono rispettare determinati criteri, inclusi la riproducibilità e la verificabilità dei risultati.

In conclusione, potremmo dire, che la prospettiva dell'attività tecnica resta quella della utilizzabilità in dibattimento delle informazioni raccolte, messe a disposizione di tutte le parti processuali per la valutazione di ogni aspetto rilevante e ciò a garanzia dell'esercizio del diritto di difesa e a salvaguardia dei diritti fondamentali dei soggetti coinvolti.

Inoltre, ciò che si vuole evitare è che le indagini si trasformino in «vere e proprie incursioni investigative nel nucleo più intimo dell'individuo»[96].

9 Bibliografia

Antolisei F., *Manuale di diritto penale, Parte generale*, Giuffrè, 1987.

Aterno S. - Cajani F.- Costabile G. - Mattiucci M. - Mazzaraco G., *Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Experta, Milano, 2011, p. 411.

Aterno S., Mazzotta P., *La perizia e la consulenza tecnica – con approfondimento in tema di Perizie Informatiche* (analisi e schede tecniche di Caccavella D.), CEDAM, 2006.

Bardari U., *L'esperimento giudiziale su posizionamento GPS e scatole nere per automobili*, in Brighi R., Palmirani M., Sánchez Jordán E. (a cura di), *Informatica giuridica e informatica forense al servizio della società della conoscenza*, Aracne, 2018.

Bartoli L., Maioli C., *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in Biasiotti M. A., Epifani M., Turchi F. (a cura di), *Trattamento e scambio della prova digitale in Europa*, Edizioni Scientifiche Italiane, 2016, pp. 139-151.

Bassini M., *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in Quad. cost., settembre 2016.

Berghella F. – Blaiotta R., *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen*. 1995, p. 2329.

Bragò G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in L. Luparia, Sistema e criminalità informatica, Giuffrè, Milano, 2009.

Bravo F., *Crimini informatici e utilizzo dei mezzi di ricerca della prova nella conduzione delle indagini*, in *Riv. giur. polizia*, 1998, p. 711.

Brighi R., *Informatica forense, algoritmi e garanzie processuali*, 2001.

Brighi R., *Sfide recenti e nuovi paradigmi dell'Informatica forense*, in *nuove questioni di informatica forense*, Aracne, Roma, 2022.

Buffa F., *Internet e criminalità*, Milano, 2001.

Cajani F., Aterno S., *Aspetti giuridici comuni delle indagini informatiche*, in Aterno S., Cajani F., Costaile G., Mattiucci M., Mazzaraco G. (a cura di), *Computer forensics e indagini digitali*, Experta, Milano, 2011.

Calabrò S., *Mobile device and mobile cloud computing forensics*, Torino, 2016.

Carnevale S., *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, Negri D. - Carnevale S. - Addis M. P. (a cura di) *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Aracne, Roma, 2007

96. Così si esprime R. Orlandi in *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, Riv. it. dir. proc. pen., 2018, 2, p. 539.

Casey E., *Digital Evidence and Computer Crime. Forensics science, computers and the Internet, Elsevier*, 2004, p. 1.

Casey E., *The value of forensic preparedness and digital-identification expertise in smart society*, in Digital investigation, 2017, 22, pp.1-2.

Caviglione L., Wendzel S., Mazurczyk W., *The Future of Digital Forensics: Challenges and the Road Ahead*, in IEEE Security & Privacy, 2017.

Corona F., *Le attività di digital forensics nel cybercrime, in Reati informatici e investigazioni digitali,* Pacini Giuridica, 2002.

Costabile G., *Computer forensics e informatica investigativa alla luce della legge n. 48 del 2008, in Ciberspazio e diritto*, 2010.

Costabile G., *Indagini digitali*, in Aterno S., Cajani F., Costabile G., Curtotti D. (a cura di), *Cyberforensics e indagini digitali*, Giappichelli, 2021.

Hopper L. C., Martin B., Raymond Choo K.K., *Cloud Computing and Its Implications for Cybercrime Investigations in Australia, in Computer Law & Security Review*, 2013, vol. 29, p. 2;

Cuomo L. - Izzi B., *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico*, in *Cass. pen*., 2002, p.1018.

Cuomo L., *La prova digitale*, Canzio G. - Luparia L. (a cura di) *Prova scientifica e processo penale,* CEDAM, 2017.

Curtotti D., Rizzi V., Nocerino W., Russitto A.M., Giliberti G., Scarpa G., *Piattaforme criptate e prova penale*, in *Sistema penale*, Rivista, 2023.

Dal Checco P., Ripetibilità e Irripetibilità delle Acquisizioni Forensi tratto dagli Atti del Convegno della tavola rotonda su "Ripetibilità e irripetibilità delle acquisizioni forensi in ambito d'indagini digitali", Roma, 2016.

Daniele M., *Habeas corpus. Manipolazioni di una garanzia*, Giappichelli, 2017.

Demartis F., *La nuova disciplina sui tabulati: un completo adeguamento agli standard europei?*, in *Dir. pen. proc*., 2022, p. 306.

Dinacci F. R., *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *Proc. pen. giust*., 2022.

Dominioni O., *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2005.

Epifani S., *Analisi di telefoni cellulari in ambito giuridico, relazione all'Incontro studi sul tema «Scienze e processo penale»,* Roma, 27-29 giugno 2011, in www.csm.it.

Ferrazzano M., *Dai veicoli a guida umana alle autonomous car. Aspetti tecnici e giuridici, questioni etiche e prospettive per l'informatica forense*, Giappichelli, 2018.

Filippi L., *Il rilevamento del tracciato axe: una nuova denominazione per una vecchia indagine*, in *Giur. it*., 1999, p. 1687.

Frank R., *Tutela della riservatezza e sviluppo tecnologico*, in *Giust. civ*., 1987.

Frosini V., *I calcolatori elettronici e il nuovo mondo civile, in «Rivista internazionale di filosofia del diritto», 4, 1973, p. 704 ss.; Id., La giuritecnica: problemi e proposte, in «Informatica e diritto», 1, 1975, p. 26 ss., Id., Informatica diritto e società, Giuffrè, Milano, 1988; Id., La giuritecnica: problemi e proposte, in «Amministrazione e politica», 3, 1976, p.187 ss.*

Frosini V., *La protezione della riservatezza nella società informatica*, in Matteucci N. (a cura di), "*Privacy e banche dei dati"*, Bologna, Il Mulino, 1981, 37 ss; ID., in *questa Rivista*, 1981, n. 1, p. 5 ss.; ID., *Informatica diritto e società*, II ed., Milano, Giuffrè, 1992, p. 173 ss.

Galdieri P. *Il domicilio informatico: l'interpretazione dell'art. 615-ter cod. pen. tra ragioni di carattere sistematico e forzature*, in *Diritto inf.,* 2013.

Galli R., *Alcune note sulla «privacy» (legge n. 675 del 1996)*, in *Foro pad*., 1998.

Gallo N., *L'acquisizione del traffico telefonico nelle indagini di polizia*, in Riv. di polizia, II, 2008.

Gammarota A., Caccavella D., *L'informatica forense per l'E-Health*, in Faralli C., Brighi R., Martoni M. (a cura di) *Strumenti, diritti, regole e nuove relazioni di cura. Il paziente europeo protagonista nell'eHealth*, Giappichelli, 2015.

Ghirardini A., Faggioli G., *Computer Forensics*, Giappichelli, 2007.

Golin S., *Questioni aperte sull'acquisizione probatoria di dati informatici (*a cura di) Brighi., *Nuove questioni di informatica forense*, Aracne, Roma, 2022.

Grippo V., *Analisi dei dati personali presenti su Internet. La legge n. 675/96 e le reti telematiche*, in *Riv. critica dir. priv*., 1997, p. 639.

Iaselli M., *Investigazioni digitali*, Giuffrè Francis Lefebvre, 2020.

Librando V., *La tutela della riservatezza nello sviluppo tecnologico*, in *Dir. inf. e informatica*, 1987, p. 487.

Luberto M. – Zanetti G., *Il diritto penale nell'era digitale. Caratteri, concetti e metafore*, in *Indice pen*., 2008.

Ludovici L., *I criptofonini: sistemi informatici criptati e serverocculti,* in *Penale DP*, Rivista, 2023.

Luparia L., Ziccardi G., *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007.

Maioli C., *Dar voce alle prove: elementi di informatica forense,* in P. Pozzi (a cura di) *Crimine virtuale, minaccia reale*, Franco Angeli, 2004.

Maioli C., Sanguedolce E., *I nuovi mezzi di ricerca della prova fra informatica forense e L. 48/2008*, Altalex, 7/5/2012.

Mantovani F., *Diritto Penale, Parte generale*, Cedam, 1992.

Marafioti L., *Digital evidence e processo penale*, in *Cass. pen*., 2011.

Mattiucci M., *Il digital forensics: dal computer al cellulare, ad internet fino all'elettronica pura*, in Sicurezza e Giustizia, n. IV/MMXI, 50.

Mucciarelli F., Commento alla legge 23 dicembre 1993 n.547. *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, in Leg. Pen., Utet, Torino, 1996.

Murro O., *Lo smartphone come fonte di prova. Dal sequestro del dispositivo all'analisi dei dati*, CEDAM, 2024.

Murro O., *Dubbi di legittimità costituzionale e problemi di inquadramento sistematico della nuova disciplina dei tabulati*, in *Cass. pen*., 2022.

Nocerino W., *L'acquisizione della messaggistica su sistemi criptati: intercettazioni o prova documentale?*, in *Cass. pen*., 2023, p. 2786.

Orlandi R. in *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, Riv. it. dir. proc. pen., 2018, 2, p. 539.

Parlato L., *Libertà della persona nell'uso delle tecnologie digitali*, in *Associazione tra gli studiosi del processo penale, Diritti della persona e nuove sfide del processo penale*, Giuffrè Francis Lefevre, Milano 2019.

Perri P., *Computer forensics (indagini informatiche)*, in *AA.VV*., Dig. pen., Utet, IV Agg., 2011.

Picotti L., *Ratifica alla Convenzione cybercrime e nuovi strumenti di contrasto alla criminalità informatica e non solo*, in Diritto dell'internet n. 5, Ipsoa, Milano, 2008.

Pichan A., Lazarescu M., Soh S. T, *Cloud Forensics: Technical Challanges, Solutions and Corporative Analysis*, in Digital investigation, 2015.

Raghavan S., *Digital Forensic Research: Current State of Art,* in *CSI transactions on ICT*, 2013, n. 1.

Riccobono F., *La filosofia del diritto di Vittorio Frosini dalla morfologia della prassi all'informatica giuridi*ca, in Charalambis D., Papacharalambous C. (Hrsg. von), *Jus, ars, philosophia et historia. Festschrift für Johannes Strangas*, Nomos, Baden-Baden 2017.

Rodotà S., *Il mondo della rete. Quali vincoli, quali diritti*, Laterza, Roma 2014.

Rodotà S., *Libertà personale. Vecchi e nuovi nemici*, Bovero M. (a cura di) *in Quale libertà. Dizionario minimo contro i falsi liberali*, Laterza, 2004, p. 52.

Rodotà S., Una scommessa impegnativa sul terreno dei nuovi diritti, *InterLex Diritto Teconolgia e Informazione,* 2002, http://www.interlex.it/675/rodota6.htm.

Romeo F., *Habeas Data*, la forza normativa di un'idea, D'Avack, Faralli, T.E. Frosini, Jellamo, Andrini, Riccobono, Limone, Romeo, Caridi, Ciacci, Punzi (a cura di) in *Vittorio Frosini: una coscienza giuridica aperta al futuro, Rivista internazionale di filosofia del diritto,* Giuffrè Francis Lefebvre, 2019.

Serra C., Strano M., *Nuove frontiere della criminalità*, Milano, 1997.

Signorato S., *Data retention, tra diritto alla protezione dei dati personali ed esigenze di accertamento dei reati*, Brighi R. (a cura di), *Nuove questioni di informatica forense*, Aracne, Roma, 2022.

Signorato S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, p. 75.

Signorile O., Computer Forensic Guidelines: *un approccio metodico-procedurale per l'acquisizione e analisi delle digital evidence*, in Ciberspazio e Diritto, Mucchi editore, Modena, 2009.

Tonellotto M., *Evidenza informatica, computer forensics e best practices*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, 2014.

Valastro A., *La tutela penale delle comunicazioni intersoggettive, fra evoluzione tecnologica e nuovi modelli di responsabilità*, in *Riv. it. dir. e proc. pen*., 1999.

Ziccardi G., *Informatica giuridica*, Giuffrè, Milano, 2006.

Zuboff S., *ll capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, tradotto da Bassotti P., Luiss University Press, Roma 2019.